FULL DISCLOSRE OF COMPUTER SECURITY VULNERABILITIES: AN EXAMINATION OF THE DEBATE

by

Tami Marie Goens

An Undergraduate Distinction Project Presented in Partial Fulfillment of the Requirement for Graduation with Distinction in the College of Business at The Ohio State University

BSBA Accounting Honors & MIS with Distinction

The Ohio State University

2001

Distinction Examination Committee:

Dr. Richard Murdock, Advisor
Dr. Daniel Jensen
Dr. John Butler

Approved by

Advisor
Department of Accounting & MIS

ABSTRACT

BugTraq, a popular mailing list now hosted by securityfocus.com, was founded in 1993 to provide a forum for open publication of computer and network security vulnerabilities. Due primarily to the rapid pace of software development and the proliferation of the Internet, there has been a shift away from keeping computer security vulnerabilities private. Prior to such mailing lists as BugTraq, information on computer and network security vulnerabilities remained in the hands of a few, primarily computer security researchers and the underground criminal element. Retaliation to this form of private information has led many working in computer security to adopt what has become known as full disclosure. The practice of publicly disclosing computer security vulnerabilities has led to a heated debate, as there are both positive and negative consequences of releasing such information to the masses.

The goal of this distinction project is to determine the attitudes that those in the computer security community currently hold regarding issues surrounding full disclosure. Two hypotheses are tested. First, a majority of those in the computer security field support the full disclosure model of disseminating vulnerability information and second, attitudes on the full disclosure debate will vary across participation in different computer security circles. In order to test these hypotheses, opinions from users of full disclosure information and computer security practitioners were solicited through use of an on-line survey. Survey links were distributed through the FBI-coordinated computer security organization, InfraGard, the Information Systems Security Association, and the popular full disclosure mailing list, BugTraq.

ACKNOWLEDGEMENTS

I would like to thank Professor Richard Murdock for his support and guidance. He has been instrumental in introducing myself and many students before me to the world of academic research. As I am positive no other student distinction project has sent the FBI after him, I can only hope that Professor Murdock enjoyed the departure I took from accounting to computer security. My appreciation also goes out to Professor Jensen for his guidance during my undergraduate career and to Professor Butler for his willingness to serve on the distinction committee. This project would not have been possible without the help from the following individuals: Brian Wilson, Tao Wang, Stephen Flowers, Bill Yang, and Steve Romig. I'd also like to thank Amy Kuck and Anup Madampath for their support and invitation to travel the world after graduation. Lastly and most importantly, I'd like to thank my parents for everything they have done for me. Mom and Dad, this project is for you.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

Introduction

Hackers deface websites, shut them down, steal credit card numbers, and carry out other mischievous activities. However, these types of computer security problems are not necessarily those that demand technical solutions. For example, security consultant Marcus Ranum delivered a keynote address, titled "Script Kiddiez Suck" at DEF CON 8.0, the world's largest annual hacking convention. In a gutsy move, Ranum told a roomful of his peers and others attending the hacking convention that they had better change their ways. More specifically, Ranum issued a call to change the way detailed computer security information is publicly released.

Those in the computer security community were told that when they find vulnerabilities, or holes in computer systems, they should think twice about telling the world these vulnerabilities exist. Furthermore, telling everyone how to exploit the known vulnerabilities, and thus making it easier for less skilled persons (script kiddies) to attack computer systems, is a practice that is harming the computer security community and one that Ranum predicts won't be tolerated much longer. His prediction is that in the next few years, individuals who distribute such information will find themselves targets of civil lawsuits.

As an increasing number of home systems are connected to the Internet with broadband connections, IS Departments are not the only ones being victimized by invasive hackers. According to Ranum, "Joe Average" is finding himself the target of

hacking attacks and "is starting to wake up and realize hackers and script kiddies are not his friend."

Our Vulnerability

Computer software is not perfect. Estimates of the number of bugs in software range from 5 to 15 bugs per thousand lines of code (Schneier, c 336). To put this into perspective, consider that Microsoft's Windows 2000 operating system has between 35 and 60 million lines of code (Schneier, c 210). Noting a trend towards increased complexity in source code, security expert and author Bruce Schneier stated, "A more complex system is less secure on all fronts. It contains more weaknesses to start with, its modularity exacerbates those weaknesses, it's harder to test, it's harder to understand, and it's harder to analyze" (Schneier, c 357). These weaknesses, or inherent bugs in software, may leave systems open to attack and are therefore commonly referred to as *computer security vulnerabilities,* or simply *vulnerabilities.*

Individuals with malicious intentions (often referred to as blackhat hackers) may take advantage of vulnerabilities to compromise data confidentiality, integrity, and authentication. Security in the digital world seeks to ensure that only the people intended to see data have access to data (confidentiality), the data is not maliciously transformed in any way (integrity), and the person or program that created the data is genuine (authentication). When security is successfully compromised, the resulting security breach may cause devastating losses. For example, an annual joint survey conducted by the Computer Security Institute and FBI reported in the year 2000, an astounding 42% of survey respondents could quantify the losses due to computer crime. The most serious

financial losses reported were those occurring from compromises of data confidentiality, which resulted in theft of proprietary information.

Vulnerabilities in today's software products open the floodgate for malicious abuses of systems and computer crime. Corporation XYZ running a web server with a known vulnerability essentially lays down a welcome mat for many breaches of security, including site defacement or a denial-of-service attack[1]. These security problems will continue to plague Corporation XYZ until the web server vulnerabilities are effectively addressed. For example, a discovered vulnerability in Microsoft's Internet Information Server left approximately 90 percent of all web servers running on Windows NT machines wide open to attacks (McGraw).

Common Vulnerabilities

Software vulnerabilities are not a new phenomenon. Often, the same types of vulnerabilities are found and exploited. For example, buffer overflows are the most common form of security vulnerability in the last ten years (Schneier, c 207). Buffer overflows are often prevalent because they result from a lack of programmer ingenuity and diligence to take security as well as functionality into consideration when coding.

Buffer overflows are inherently present in software written in C and C++, while more modern programming languages such as Java are immune to the problem (McGraw). Every program needs a place to store bits and most computer programs create sections in memory for information storage. The C programming language allows programmers to create storage at run-time, in memory regions known as buffers. If a programmer writes more data onto a buffer than it has room for, the extra data must go

[1] A denial-of-service attack is when communication ports and memory buffers are flooded to prevent legitimate network traffic from passing through.

somewhere, thus causing a potential security problem. The excess data resulting from a buffer overflow may overwrite other data and potentially change some security critical parameters. Security experts Gary McGraw and John Viega provide a scenario to demonstrate the implications of a simple buffer overflow:

> In the simplest case, consider a Boolean flag allocated in memory directly after a buffer. Say that the flag determines whether or not the user running the program can access private files. If a malicious user can overwrite the buffer, then the value of the flag can be changed, thus providing the attacker with illegal access to private files.

The Morris worm[2] of 1988 is a famous example of how a buffer overflow was used to cause serious wide-spread damage. The worm exploited a buffer overflow in the UNIX fingered program, which returns the identity of a user when asked. This program accepts a variable containing the identity of a user as input. However, the size of the input was not limited, allowing a buffer overflow exploit. Input larger than 512 bytes overflowed the buffer and Morris wrote a specific large input that allowed the malicious program to execute as root[3] and install itself on the new machine. Proliferating this was a typo in the programming code that made the worm copy itself not once, but indefinitely, on computers connected to the Internet. The result was that computers infected by the worm crashed, leaving over 6,000 disabled servers, which represented 10% of the Internet at that time (Schneier, c 209).

Vulnerabilities based on the failure to validate user inputs are also common. When a program neglects to check input to make sure it is syntactically correct, certain

---

[2] A worm is a malicious software program that self-replicates, moving across computers on a network.
[3] On a UNIX-based system, a user with root access has the power to add, delete, or modify any file residing on the system. Authors of the widely-read computer security book, *Hacking Exposed,* state "[in] UNIX there are two levels of access: the all-powerful root and everything else. There is no substitute for root!" (Kurtz, McClure, Scambray 306). Once root access is gained, it effectively means, "game over" in the battle to maintain secure systems.

modules in the program may fail, creating field-value correlation errors. Authors of *Hacking Exposed* detail one example of an input validation attack:

> PHF is a Common Gateway Interface (CGI) script that came standard with early versions of Apache web server and NCSA HTTPD. Unfortunately, this program did not properly parse and validate the input it received. The original version of the PHF script accepted the newline character (%0a) and executed any subsequent commands with the privileges of the user ID running the web server...In most cases, the user ID was "nobody," but there were many unfortunate sites that committed the cardinal sin of running their web server with root privileges...and many sites were compromised as a result of this simple but effective exploit. (Kurtz, McClure, and Scambray 316,317)

Learning of vulnerabilities in specific software and hardware products can be thought of as the first step in carrying out a breach of security. One must first know the vulnerabilities of a system in order to exploit them. How information on these vulnerabilities is disseminated plays an important factor in the fight to effectively maintain secure computer information systems. Therefore, the release of vulnerability information and the responsibilities of those that discover these vulnerabilities is the main focal point of this study.

The Full Disclosure Movement

Computer security vulnerabilities are discovered everyday by security researchers (in academia and industry), product customers, and hackers possessing general curiosity or criminal intent. When a vulnerability is found, the discoverer has several options. He can do nothing, thereby keeping knowledge of the vulnerability to himself. He can tell his colleagues and friends about the vulnerability. He can contact the vendor of the product. In contacting the vendor, the discoverer may chose to explain the vulnerability that he found by providing detailed documentation on how he found it. Furthermore, the

discoverer may work with the vendor in order to produce a fix[4] for the vulnerability. If the vulnerability is potentially big news, the discoverer may want to alert the media to draw attention to his hacking acumen or to cause negative publicity for the vendor of the vulnerable product. The discoverer may also alert certain computer security organizations or tell the whole world, in a practice known as *full disclosure.*

Full disclosure has gained momentum in recent years, as evidenced by an increasing number of publication venues containing vulnerability information. Following is a brief continuum of the sources of vulnerability information, starting with CERT, a tightly controlled medium for vulnerability information, and ending with BugTraq, the most popular avenue for disclosing computer security vulnerabilities.

CERT

Subsequent to the Morris worm of November 1988, The Computer Emergency Response Team, more commonly referred to as CERT, was created to address computer security concerns. CERT, housed in the Software Engineering Institute of Carnegie Mellon University, primarily handles incident and vulnerability reports, forming a network of key contacts to respond to computer security emergencies. CERT will respond 24 hours a day to organizations that report compromised security. The organization also serves as a "focal point for the research community for identification and repair of security vulnerabilities, informal assessment of existing systems in the research community, improvement emergency response capability, and user security awareness" (Carnegie Mellon University Press Release).

[4] A fix is a software patch issued by the vendor or some other type of workaround solution to eliminate the particular vulnerability.

A total of 774 vulnerabilities were reported to CERT in 2000, which led to the publication of 22 CERT advisories (CERT). CERT does not publicly release information on all of the vulnerabilities known to the organization. Rather, CERT follows a set of procedures for releasing information on computer security vulnerabilities. It established a new vulnerability disclosure policy that became effective October 9, 2000. Previously, CERT would only release information on a vulnerability if a fix to the vulnerability was found. The impact of this procedure, as evidenced above, is that CERT would not publicly release information on a great number of vulnerabilities known to it. However, the new policy states that in most cases, CERT will release reported vulnerabilities 45 days after the organization receives the initial report, regardless of whether a fix has been established. Therefore, under the new policy, one can expect the number of published CERT advisories to climb.

CERT publishes advisories to its mailing list and on the Web. However, the advisories are limited to the vulnerabilities that CERT evaluates to meet a certain threshold for severity. Additionally, CERT publishes "CERT Vulnerability Notes," which is a searchable database of vulnerability information, similar to the advisories, but which "may have less complete information" (CERT).

Many working in computer security did not feel CERT was an effective provider of computer security vulnerability information. It was perceived as being slow to confirm vulnerabilities because CERT would communicate with vendors until a fix was available before releasing any information to the public. Many users believed that vendors were slow to respond because they had no incentive to produce quick solutions. Furthermore, according to widely published computer security consultant, Bruce

Schneier, "CERT was slow about publishing reports even after the fixes were implemented" (Schneier, c 339).

Guarded security information did not sit well with those desiring more timely information regarding known vulnerabilities. For example, consider the scenario of a vulnerability, already known to the criminal hacking element, which is reported to CERT. System administrators dependent on CERT for vulnerability information would not be made aware of the vulnerability until it has gone through CERT's clearing process. While system administrators are kept in the dark regarding the vulnerability, the attacker may exploit at will until the vulnerability is patched. Scenarios such as this demonstrate the need for timely vulnerability information in order for it to be effective in preventing attacks. As CERT is organized primarily to respond to incidents after the fact, many consider the organization's model of vulnerability disclosures to be ineffective in the prevention of attacks. Therefore, the belief that vulnerability information should be made available to the public shortly after discovery stirred a shift towards other models of disclosing vulnerabilities.

BugTraq

BugTraq, a subscription-based electronic mailing list founded in 1993, is a popular distribution channel for the latest computer security vulnerability information. BugTraq subscriptions are open to anyone with an e-mail address and number approximately twenty-seven thousand subscribers. One of the founders of SecurityFocus.com, the organization now hosting BugTraq, explains, "BugTraq was designed from the start as an open forum for the no-holds-barred discussion of security vulnerabilities" (Rauch).

The BugTraq model works in the following manner. Someone reports a vulnerability to BugTraq by sending an e-mail message to the BugTraq list. The list moderator approves the posted message to ensure it stays on the topic of computer security vulnerabilities. After approval, the message containing the reported vulnerability is sent via e-mail to every BugTraq subscriber. Under the BugTraq method for disclosing vulnerabilities, the process from reporting a vulnerability to publication may only take seconds. The reported vulnerabilities are not confirmed for technical merit or held for specific periods of time, such as the case with the CERT model. E-mails posted to BugTraq may contain a brief description of a new vulnerability, step-by-step instructions of how to exploit or fix the vulnerability, or announcement of an automated attack tool to exploit the vulnerability. As will be discussed further, mailing lists such as BugTraq are controversial because information on vulnerabilities is released to those with malicious intentions before fixes are available.

Full Disclosure Debate

The full disclosure debate is essentially an argument of how to best minimize the window of exposure to computer security vulnerabilities. Bruce Schneier has coined the term "window of exposure" to describe the time until a patch for a vulnerability becomes available and users of the vulnerable product apply the patch. Figure 1 illustrates the window of exposure. The risk implied on the vertical axis refers to the risk that a malicious user will exploit the vulnerability. Note that this risk increases as the vulnerability becomes public knowledge and decreases after users fix their systems (through application of the vendor patch).

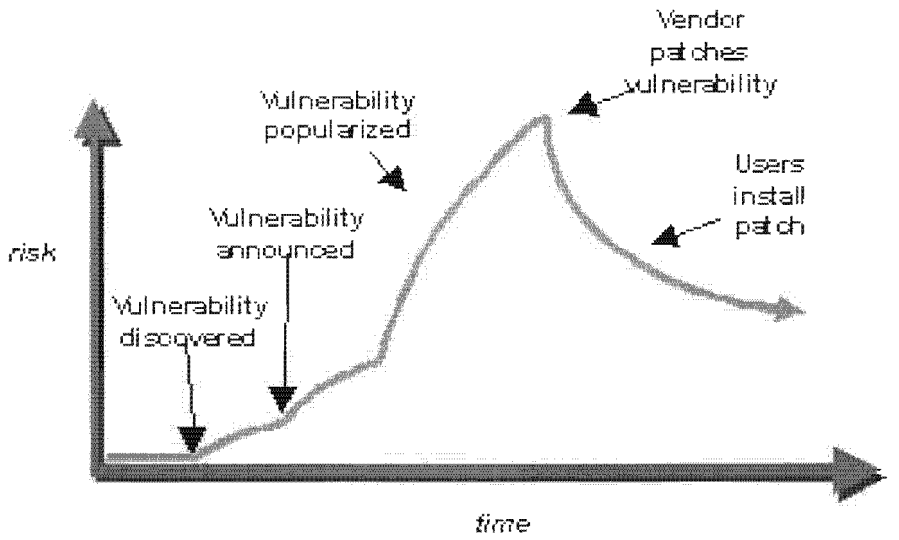


Figure 1

(Schneier, a)

System administrators should patch vulnerabilities before attackers can take advantage of them. However, if an easy-to-follow vulnerability exploit script is posted to BugTraq, malicious users everywhere are able to do some damage before the system administrator knows what hit him. On the other hand, the published vulnerability exploit code will pressure the vendor to fix the problem fast, enabling users of the vulnerable product to protect themselves. Therefore, the dilemma is somewhat of a race to see who will use the vulnerability information first to an advantage--the good guy or the bad.

Pro

A quote dating back to the 1850s has been used in computer security publications to represent the argument for full disclosure (Schneier, b). In his *Rudimentary Treatise on the Construction of Locks*, Charles Tomlinson writes:

"In respect to lock-making, there can scarcely be such a thing as dishonesty of intention: the inventor produces a lock which he honestly thinks will possess such and such qualities; and he declares his belief to the world. If others differ from him in opinion concerning those qualities, it is open to them to say so; and the discussion, truthfully conducted, must lead to public advantage: the discussion stimulates curiosity, and curiosity stimulates invention. Nothing but a partial and limited view of the question could lead to the opinion that harm can result: if there be harm, it will be much more than counterbalanced by good."

While not proven to exist, many perceived benefits may arise from the public dissemination of vulnerability information. When a vulnerability is made public, the vendor of the vulnerable product is pressured to produce a quick fix or face losing the satisfaction of its customers and confidence of the public. When the world knows about a vulnerability, the vendor will be more likely to produce a fix faster than if the vulnerability was kept private. Users of the vulnerable product are likely to anticipate a fix, and will apply the vendor patch or implement a work-around solution to address the problem. Therefore, supporters of the free flow of vulnerability information believe that "security is getting better a lot faster because of full disclosure" (Schneier, c).

The person that publicly posts a vulnerability may not be the first person to discover it. Blackhat hackers may have previously known about the vulnerability; thus full disclosure is arming the security community with the same information. Therefore, full disclosure increases the likelihood that system administrators can defend their systems against attack. Keeping vulnerabilities a secret from the computer security community could be effective if the vulnerability truly remains a secret and those with malicious intentions never discover the vulnerabilities. However, as there are extremely skilled persons with the motivation to discover vulnerabilities, openly discussing these vulnerabilities will lead to more robust software and hardware. Bruce Schneier explains, "By aligning yourself with the natural flow of information instead of trying to fight it, you end up with more security rather than less" (Kurtz, McClure, Scambray xviii).

Full disclosure supporters often present a scenario about what would happen without the free flow of computer security information. A fear exists that without full disclosure, vulnerability information would be pushed underground (McClure). This

keeps the information out of the hands of the system administrators that need it. Therefore, the security researchers in academia and blackhat hackers would serve as keepers of vulnerability information. Furthermore, information on how to exploit vulnerabilities would be traded among those with the resources and connections to do so, creating private exploitation.

Evidence from the Computer Security Institute/FBI annual survey suggest that organizations are experiencing an increased number of attacks since full disclosure has become popularized. It should be duly recognized, however, that the number of computers connected to the Internet has grown tremendously over the past few years. In 1993, three million people were connected to the Internet. By 1999, approximately 200 million people were connected worldwide (Internet Indicators). Therefore, an increase in the number of attacks may be partially attributed to the exponential growth of the Internet.

Full disclosure itself does not cause computer security vulnerabilities. Vulnerabilities exist because software and hardware developers are not as diligent as they should be when testing for security and because it's near impossible to produce 100% secure products. Security researcher Juan Carlos Cuartango reported a security flaw in Microsoft's Internet Explorer 5 (IE5) only one week after its release. He discovered that the browser could allow websites to read the contents of a web surfer's clipboard. Meanwhile, another security researcher, George Guninski, discovered three other flaws that could allow someone to have unauthorized access to files on the system running IE5 (Spanbauer). Because every piece of software ships with some embedded vulnerabilities,

full disclosure may be viewed as the messenger service for reporting these vulnerabilities, and not the cause of the vulnerabilities themselves.

Con

While full disclosure aids those responsible for maintaining the security of computer systems, it also arms those with less noble intentions. After all, it is impossible exploit a vulnerability one does not know about. On this, Bruce Schneier, in the forward to *Hacking Exposed*, writes:

> A network with a security vulnerability is insecure to those who know about the vulnerability. If no one knows about it—if it is literally a vulnerability that has not been discovered—then the network is secure. If one person knows about it, then the network is insecure to him but secure to everyone else. If the network manufacturer knows about it...if security researchers know about it...if the hacking community knows about it--the insecurity of the network increases as news of the vulnerability gets out (Kurtz, McClure, Scambray xvii).

Simply put, full disclosure allows information critical to upholding security to reach the wrong users. Individuals desiring to cause trouble may use full disclosure announcements to learn about vulnerabilities and how to write attack programs. Especially dangerous are point-and-click attack programs made available to take advantage of certain vulnerabilities. Automated attack tools allow script kiddies to break into systems when without the attack tool, they lack the technical skill to perform such a feat.

Releasing information concerning a vulnerability leaves effected systems vulnerable to additional attackers until a patch is produced. Furthermore, an available patch does not solve the problem until it is properly applied to the vulnerable system. For multiple reasons, organizations don't always keep up with the latest patches for their systems. Therefore, many believe that full disclosure increases the risk that vulnerable

systems will be compromised as more people become aware of the vulnerability and details on how to exploit the vulnerability become available.

Those against full disclosure do not believe the practice is beneficial to the computer security community because software and hardware vendors are not learning from their mistakes. Vulnerabilities are still caused by buffer overflows and invalidated user input, among other known problems. In his hacking convention speech, Marcus Ranum noted that 99% of the bugs found fall into well-known flaw taxonomies.

Ranum also addressed other "myths of full disclosure." According to Ranum, while hackers may already know about vulnerabilities prior to their disclosure, script kiddies did not. Furthermore, he does not believe the argument that vendors can't hide when the public knows their products are vulnerable. Ranum pointed out that the hacking group, l0phtcrack, has published problems with Microsoft's Windows operating system for which Microsoft has yet to produce a solution. Ranum also sees full disclosure as a tool for self-promotion. He told the audience "many of the vulnerabilities being disclosed are researched and discovered for the *purpose* of being disclosed."

Significance of the Problem

As more people use the Internet and society becomes increasingly dependent on technology, issues of computer security demand increased attention. More security breaches are being reported to law enforcement officials (CSI/FBI). Both government and the private sector are searching for ways to minimize the losses from breaches of computer security. The full disclosure debate provides important dialog on the best way to improve the state of computer security. In addition, the full disclosure debate raises the problem in the definition of ethical behavior in the wake of discovering security

vulnerabilities. The attitudes of the computer security community on the full disclosure issue are significant in the sense that secure computer systems have become increasingly important for many organizations and individuals.

CHAPTER 2

REVIEW OF RELATED LITERATURE

Introduction

Little research exists on the subject of full disclosure. Perhaps because the full disclosure phenomenon is a relatively new, writings on the subject consist mostly of articles and editorials posted to e-mail lists and websites. A few have attempted to tackle some of the specific issues involved. While not conducted in an academic setting, the following writings indicate important implications to the full disclosure debate.

Applying Patches to Known Vulnerabilities

Computer security consultant Dan Farmer conducted a security survey in late 1996 to profile Internet systems that contained exploitable vulnerabilities. While the study was conducted independently, without the utilization of scientific methodologies, the results are nevertheless significant. Using non-intrusive techniques, Farmer found that nearly two-thirds of the Internet systems he scanned contained potential security vulnerabilities (Farmer). Automated scanning software was used to look for vulnerabilities previously published in CERT advisories. In other words, systems were found to be vulnerable because administrators did not fix known vulnerabilities by applying the latest patches to their systems.

Full Disclosure and Website defacement

Attrition (http://www.attrition.org), is a group that collects and distributes information on security advisories, cryptography, text files, and denial of service attacks. It is popularly known for having the largest mirror of website defacements. Using data from Attrition and BugTraq archives, security engineer Brian Martin has written on the cause and effect relationship between the release of exploit code and website defacements. Martin traced eight vulnerabilities and the date the exploit code associated with them was fully disclosed to BugTraq. The eight examples demonstrated that the number of website defacements tend to increase after the disclosure of exploit code.

While data pointed to the conclusion that publicizing exploit scripts leads to more security breaches, Martin notes that this may not be the case. "One must consider the sequence of events and results of exploits being created but *not* being posted to a public forum. Unpublished exploit scripts are like currency in the hacker subculture. The power of a single remote exploit that is unknown to vendors enables a single person to potentially break into thousands of machines, often with no recognizable trace of how it was done...In some cases, these exploits circulate in the underground for up to a year before being made public." (Martin).

Policy for Full Disclosure

A computer security consultant known as "Rain Forest Puppy" (commonly referred to as FRP), introduced a policy for those who discover vulnerabilities. FRPolicy v2.0 is made available on-line to provide guidance on how to best communicate with vendors prior to disclosing a vulnerability. In his policy, RFP reminds software vendors

that those who report vulnerabilities to them have chosen not to immediately disclose the problem. Therefore, vendors are encouraged to provide an efficient response to the person who reported the vulnerability. The person who reported the vulnerability is advised to give the vendor five working days to respond before posting the information to a public disclosure forum. The person reporting the vulnerability should be willing to provide information on how to reproduce the vulnerability if requested by the vendor. FRPolicy v2.0 encourages the vendor and person reporting the vulnerability to "coordinate a joint public release/disclosure" (FRP). In addition, the policy dictates that the vendor should recognize proper credit to the person reporting the vulnerability.

Difficulty in Conducting Controlled Experiments

There is no evidence to concretely prove the effects of full disclosure. There are many difficulties in conducting experiments in the sensitive arena of computer security. First, system administers are not likely to cooperate in studies that involve the technical settings of their systems. Additionally, many organizations are even reluctant to report computer crimes to law enforcement officials (CSI). Dr. Gene Spafford, a researcher with the Purdue University CERIAS lab (http://www.cerias.purdue.edu/), posted to the BugTraq mailing list a scenario for how one may test the effects of full disclosure on vendor responsiveness.

"If one wanted to do a controlled set of trials (once is not sufficient for meaningful comparison; staff absence, illness, holidays, etc could be confounding effects), one would need to do something like:

1) pick N bugs of roughly similar impact, severity, and type.
2) randomly, over time, release N/2 as full disclosure, and the other N/2 as private communications to the vendor(s).
3) time and evaluate the responsiveness of the vendors to these events.
4) don't let the vendors know they are being tested" (Spafford).

Such a controlled study has yet to be conducted regarding the effects of full disclosure. On the dangers of this, Dr. Spafford has commented to the BugTraq list,

> "My key concern is that people on the net, and on these lists in particular, spout opinion as proven fact. This perpetuates folklore, just as knocking on wood or avoiding black cats. We have no general evidence to prove in any real way that full disclosure helps/hurts more than it hurts/helps. We have no evidence that full disclosure hastens/delays release of a fix. And we have no evidence that the majority of "black hats" know and use all of these flaws before they are publicly announced...If we are going to improve the way we handle security, we have to start by examining what we really know and not what we have experienced locally" (Spafford).

Implications for This Study

Since it is extremely difficult to conduct controlled experiments to prove the effects of full disclosure, this study will concentrate on the current perceptions of those interested in computer security. Most of the found literature regarding full disclosure is supportive of its cause, with the notable exception of articles and addresses from security consultant, Marcus Ranum. Therefore, the study proposes that a majority of those in the computer security field support the full disclosure model of disseminating vulnerability information. As there has been increased publicity on the issue following Ranum's hacking convention address, this study attempts to discover if attitudes regarding full disclosure vary across those in the industry.

CHAPTER 3

RESEARCH METHODOLOGY

Introduction

The purpose of this study was to determine the opinions of computer security practitioners on a range of issues related to full disclosure. Two hypotheses were tested. First, a majority of those in the computer security field support the full disclosure model of disseminating vulnerability information and second, attitudes on the full disclosure debate will vary across participation in different computer security groups. In order to test these hypotheses, opinions from users of full disclosure information and computer security practitioners were solicited. The responses can be used as an indicator for the attitudes of the computer security community regarding the full disclosure issue. A survey was distributed to three different groups of users—members of the computer security group InfraGard, members of the Information Systems Security Association, and subscribers to BugTraq. These three groups were chosen because they may have differing opinions on the issue. In addition, these three groups are likely to have a high level of familiarity with the topic in theory and in practice.

Survey Respondents

Three Groups

Full disclosure of computer and network security information is a highly specialized and complex topic. Therefore, it was necessary to send surveys to groups that have some knowledge and hands-on experience dealing with computer security vulnerabilities and the consumption of computer security vulnerability information. In

order to understand the impacts of full disclosure, a person must have a working knowledge of what computer security vulnerabilities are and understand how vulnerabilities pose a threat if exploited. A person knowledgeable about the full disclosure issue must also understand the roles of the players involved, mainly computer security researchers, software users, system administrators, software vendors, blackhat hackers, script kiddies[1], etc. Surveys were distributed to InfraGard and the Information Systems Security Association, and to BugTraq, the popular full disclosure mailing list.

InfraGard

Founded in Cleveland, Ohio in 1996, InfraGard exists as a partnership between the U. S. government and private industry to promote the protection of our nation's critical infrastructures, including (but are not limited to), telecommunications, energy, banking and finance, transportation, water systems, government operations, and emergency services. The FBI and the National Infrastructure Protection Center (NIPC) represent the U. S. government in this partnership, addressing President Clinton's *Presidential Decision Directive 63*, which calls for a public-private partnership to reduce the vulnerabilities that arise from increasingly interdependent and automated computer systems (The Clinton Administration). InfraGard forms a closed circle of those working in computer security to reduce the vulnerabilities of our critical infrastructures "through

[1] A script kiddie is: 1. A computer user who utilizes the work of other more skilled people for personal gain, typically without giving anything back to the computer security community; 2. A computer user who maliciously, and without authorization, modifies the contents of Web sites; 3. A computer user who claims a higher skill level than he or she genuinely possesses
-Jay Dyson, Senior Security Consultant at OneSecure (Koch)

the referral and dissemination of information regarding illegal intrusions, disruptions, and exploited vulnerabilities of information systems" (San Francisco InfraGard).

There are fifty-six chapters of InfraGard nationwide, each associated with a FBI field office. Chapters are comprised of a representative from the chapter's local FBI field office and members from private and publicly held companies, academic institutions, and state and local law enforcement agencies, among other participants (InfraGard by-laws). InfraGard members represent a trusted group of those concerned with computer security for the betterment of society. Therefore, in order to become a member of InfraGard, one must agree to abide by a code of ethics. InfraGard members agree to restrain from participating in illegal or improper activities. In addition, InfraGard members must agree to maintain confidentiality of proprietary, confidential, or otherwise sensitive information obtained through involvement with InfraGard.

The InfraGard approach to discussing computer security issues in a closed circle serves to build trust between the InfraGard members and the FBI, benefiting both parties. Members meet on a regular basis, usually once per month, to discuss the computer security issues faced by their respective organizations. This sharing of information helps members to better prepare their own organizations against information security threats. The FBI shares information with InfraGard members about how to preserve evidence once an attack is identified, making it easier for the FBI to prosecute criminals. The grassroots approach serves to foster a cooperative relationship so that when something does go wrong, law enforcement officials can investigate and the victim organization can move on with business.

Limitations in Selection of InfraGard

One of the primary difficulties in sending out a survey to InfraGard members is the level of privacy the FBI upholds to create and maintain trust among InfraGard members. Members of InfraGard may request that their membership in the organization be kept private. Therefore, for this study, membership lists for InfraGard chapters could not be obtained. However, after a probable background check by the FBI, a listing of the FBI InfraGard coordinators was provided. Therefore, the endeavor to send a survey to InfraGard members meant obtaining approval from InfraGard chapter coordinators, most of whom are FBI Special Agents. The limitation of having the survey first go through FBI Special Agents is the possibility of a decision not to cooperate by an individual Special Agent resulting in InfraGard members never seeing the survey. The inclination of the FBI InfraGard coordinators to cooperate in this study makes it difficult to establish a survey response rate, as the bias of the InfraGard coordinators does not necessarily represent that of individual InfraGard members.

InfraGard experienced its national rollout on January 5, 2001, thirteen days before chapter coordinators nationwide were initially contacted for participation in this study. Perhaps because InfraGard has not been a national organization for very long, inconsistencies exist across chapters. For example, one InfraGard coordinator would not disclose the number of members in his respective chapter, while another provided the number of general members without specifically being asked for this information. One FBI InfraGard coordinator phoned the project advisor to explain his chapter was still in the formation stage and had yet to hold a meeting. Another chapter coordinator was

reluctant to distribute the survey to his members because the chapter was without a president and/or official spokesperson at the time of the request.

Information Systems Security Association

The Information Systems Security Association (ISSA) is an international membership organization for information security practitioners. ISSA provides, "education forums, publications and peer interaction opportunities that enhance the knowledge, skill and professional growth of its members." Members of ISSA must be employed in an information security position or be an educator, student, attorney, or law enforcement official having an interest in information security. In addition, marketers or suppliers of security products or services are permitted to join. Members must pay membership dues and agree to abide by the ISSA Code of Ethics. The ISSA Code of Ethics states that ISSA members must obey the law and "promote good information security concepts and practices," among other duties.

The ISSA is organized into chapters, located throughout the world. At present, there are ISSA chapters in twenty-eight U. S. states. Only the ISSA chapters located in the United States were surveyed to remain consistent with the InfraGard sample.

Limitations in Selection of the Information Systems Security Association

Similar difficulties to the InfraGard group exist in the selection of the ISSA as a target group. ISSA membership is not publicly available and a request for participation in this study went unanswered by the ISSA Board of Directors. Therefore, each of the ISSA chapter presidents were contacted via e-mail. The limitation of having the survey

first go through the ISSA chapter presidents is the possibility of a decision not to cooperate by the President results in members who never see the survey. The inclination of the ISSA chapter presidents to cooperate in this study makes it difficult to establish a survey response rate, as the bias of the ISSA chapter presidents does not necessarily represent that of individual ISSA members.

BugTraq

As mentioned earlier, BugTraq is a popular full disclosure mailing list that has over twenty-seven thousand subscribers. Subscribers to BugTraq receive announcements regarding computer and network security vulnerabilities for a wide range of software and hardware products. Oftentimes, BugTraq postings will consist of detailed discussions of vulnerabilities, including how to exploit them and how to fix them. BugTraq is a moderated list; therefore the moderator must first approve each posting to the list. The moderator does not verify the technical information in BugTraq postings, but rather serves to keep the discussion relevant to the full disclosure of vulnerability information.

Limitations in Selection of BugTraq

BugTraq subscription is open to anyone, including computer security researchers, system administrators, programmers, educators, hackers (whitehat, blackhat, and grayhat), and all elementary and high school children interested in causing trouble through use of a computer (often called scriptkiddies). Therefore, this group represents a lesser-controlled sample when compared to the other two membership groups with established membership requirements and whose members adhere to a code of ethics. A

subscriber to BugTraq is not necessarily trained in information security or otherwise knowledgeable to answer the survey. Furthermore, subscribers to BugTraq are likely to have the strongest opinions concerning the topic of full disclosure. BugTraq subscribers can be said to have a bias in strong favor of full disclosure since subscribers use this information and contribute to the full disclosure postings themselves. Therefore, it wouldn't be pure conjecture to say that BugTraq represents a strongly biased sample. Numerous e-mails were received commenting on the sample selection, excerpts of which are included in Appendix B, section A. Additionally, BugTraq has an international subscription base. Subscribers to BugTraq do not necessarily speak English as a first language, nor are they required to understand English at all. Therefore, it was anticipated that many BugTraq subscribers would have some difficulties understanding the survey questions due to the survey questions being authored in English. E-mails were received from foreign BugTraq subscribers who were frustrated with translating the survey questions[2].

Ballot stuffing was a great concern with the BugTraq group. It was anticipated that some curious BugTraq subscribers would answer and submit the survey more than once to see if the double counting would be allowed. Additionally, it was also anticipated that some BugTraq subscribers would submit the survey more than once in an

[2] One such e-mail reads, "The questions are hard to understand...even when translated with babel.altavista.com."

effort to discredit the results of the survey. One BugTraq subscriber sent an e-mail commenting on the possibility of ballot stuffers[3].

Because BugTraq is a moderated list, there was a risk that the survey posting would not pass through the moderator to reach subscribers. However, since the moderator approved the posting within minutes, this risk was nullified.

Limitations present in each group

There are common limitations present in each of the three groups surveyed. As previously mentioned, matters dealing with computer security issues are usually kept highly confidential. Therefore, a certain reluctance to participate in any or all computer security studies exists on the part of computer security practitioners. It would not be out of the realm of possibility for a potential survey respondent to disregard this study as part of a "social engineering"[4] attempt. In addition, opinions concerning the full disclosure issue run deep, as the issue received a great deal of publicity prior to this study. Therefore, in order for someone to respond to the survey, he/she must be interested in the full disclosure debate. In addition, those that feel the strongest about full disclosure are the ones most likely to respond to the survey, creating a self-selection bias.

---

[3] The e-mail comment reads, "I know they [the results] are not going to be scientific as you are failing to account for a number of possible injection and ballot-stuffing attacks, but they would be none-the-less interesting."

[4] Social engineering is a method whereby intruders will prey on unsuspecting employees to gain unauthorized access to computer systems. Social engineering is usually carried out when an intruder poses as a legitimate network or security administrator in order to have employees leak passwords, security configurations, or other information.

Survey Design

On-line Survey

The survey was conducted on-line through use of an html web page including a form with an associated cgi script to collect the responses. (See Appendix A for screen shots of the survey.) This was thought this to be the most effective method for data collection, considering the technology savvy-groups participating in the study. Previous surveys of computer security practitioners have been administered through regular postal "snail mail." The Computer Security Institute and the FBI conducted an annual joint security survey using the regular postal mail format and achieved a top response rate of 15% (in the 2000 survey). It was assumed that a higher number of responses would be achieved with an on-line survey because of its ease of use over a paper survey. The target survey respondents clicked an electronic link embedded in an e-mail message that directly displayed the on-line survey in a web browser. A respondent then clicked a mouse to answer the questions and to submit the survey. This method for survey submission was expected to be less time consuming for a computer literate person because locating a pen or pencil and making a trip to the post office was not needed. Furthermore, it was assumed those working in computer security were more likely to open up an on-line survey versus one contained in a paper envelope.

The e-mail messages contained a different URL (uniform resource locator or web address) for the survey based on the target group. In addition, different URLs were distributed to InfraGard and the ISSA chapters based on their geographic location within the U. S. By distributing different URLs, it was possible to trace the number of

respondents by geographic region from the InfraGard and ISSA chapters to ensure a representative sample was reached. This was done because those working in computer security may have differing opinions based on the location of their work experience. For example, a network security administrator working in the Silicon Valley region may be more security conscious than that of a network security administrator working in Alabama.

Limitations in Selection of On-line Survey

The on-line nature of this survey presented challenges to conducting a controlled experiment. Because confidentiality and privacy are often top concerns of those working in computer security, tracing individual respondents as having completed the survey was not an option. IP addresses of survey respondents can be traced without the respondents knowing the information is being collected (through use of the cgi script that is run when a respondent submits the survey). However, as this is an academic study, if IP addresses were collected, there would be an obligation to inform respondents this information was being traced. Therefore, IP addresses were not collected in an effort to ease the privacy concern of target respondents. In addition, a disclaimer was issued to inform potential respondents that the survey results were solely for use in an academic study and IP addresses would not be collected. This disclaimer was stated in the e-mail message to potential respondents and in a JavaScript pop-up dialog box. Potential survey respondents had to agree to the terms of the disclaimer in order to access the on-line survey (See Appendix A for a screen shot of the JavaScript dialog box).

As mentioned in regards to the BugTraq group, not tracing individual respondents means there is risk that the same respondent submitted the survey more than once. Furthermore, there is risk that a respondent belongs to more than one target group and thus received more than one e-mail message concerning the survey. One such respondent sent an e-mail stating he received the survey as part of his membership in two of the target groups[5].

The number of potential survey respondents that received e-mail messages containing an electronic link to the survey is unknown. As mentioned previously, some FBI InfraGard coordinators were opposed to releasing the number of members in their respective chapters. BugTraq reportedly has over twenty-seven thousand subscribers (securityfocus.com). Subscribers may add and remove themselves from the list, twenty-four hours a day, seven days a week, making it difficult to obtain the exact number of subscribers that received the survey e-mail message. All messages posted to the BugTraq mailing list are placed in the BugTraq archive (the posting for this study may be found on the securityfocus.com BugTraq Message Index from 2001-02-23 to 2001-03-01). Therefore, it's quite possible that those not subscribed to the list could have located the survey from viewing the BugTraq archive and submitted the survey as part of the BugTraq target group. In addition, those that received an e-mail message with the survey link may have forwarded the message on to others, or otherwise advertised the survey to others. A few target respondents sent e-mail messages stating they forwarded the survey

[5] The e-mail read, "I'm a member of the local InfraGard chapter and I'm also on BugTraq and several other mailing lists...Will the results of the survey be divided based on which group they were collected from?"

hyperlink to colleagues, who may or may not belong to any of the three target groups in this study.

Format of On-line Survey

The survey was authored in html and JavaScript, following the web design of the Fisher College of Business at The Ohio State University. The masthead web graphics from the academic institution were used for the survey to further add credibility to the study. The survey's appearance may have varied depending on the operating system, web browser, and monitor of the respondent. For example, a person with a seventeen-inch monitor needed to scroll through approximately five screens of questions (see Appendix A for these screen shots), whereas a respondent with a fifteen-inch monitor undoubtedly scrolled through more screens to complete the survey. Therefore, the twenty-question survey could have appeared longer to a person using a smaller monitor. The survey could have been split into several html pages to avoid this inconsistency. However, the decision was made to present all twenty questions at once so as not to appear deceptive to survey respondents.

The respondent was first presented with the JavaScript dialog box (see Appendix A, section A) to confirm agreement with the uses of the survey responses. If a respondent clicked the "Cancel" button, the potential respondent was in effect saying he/she did not agree to take the survey. A "thanks anyway" page was then displayed (see Appendix A, section C) to this potential respondent. A counter was also incremented (through use of a cgi script) to trace the number of times the Cancel button was clicked in the course of this study. It was expected that the number of times the Cancel button was

clicked is an indicator as to the level of privacy sensitivity or general paranoia regarding taking an on-line survey.

The survey itself was comprised of three parts. The first part inquired as to the respondent's background, the second part gauged the level of familiarity with current sources of vulnerability information, and the third part solicited opinions concerning full disclosure arguments. Respondents were forced to choose from a menu of responses. This was for ease of use in data collection and analysis, as the fixed-response survey also simplified the cgi script needed to collect survey responses in a readable manner. Fixed survey responses were solicited through use of radio buttons, drop down menu lists, and check boxes.

Background of Respondents

The first section of the survey asked a series of questions to gain an understanding of the general background of the respondent. The first question asked if the respondent is "responsible for computer or network security in any way." The purpose of this question was to separate those whose jobs are related to computer security from those whose jobs have nothing to do with computer security. Next, respondents were asked to select their job title from a drop-down menu list of items. The menu list of job titles was presented because there is a wide range of job titles for similar job functions across different organizations. Therefore, making respondents chose a job title that best fit their duties was an easier method for collecting and analyzing the data. An "other" list value was available for respondents who did not feel comfortable with selecting any one of the six job titles given.

Question 3 dealt with industry association. This was an attempt to gain background information on respondents and to see if those working in certain industries would have differing attitudes towards full disclosure. For example, a person employed in the financial services industry might potentially be more sensitive to the full disclosure issue because of the sensitivity of the information being processed in financial services organizations. Once again, an "other" list value was provided for respondents that felt their job does not fit within the industries listed. Respondents were asked in question 4 to select from a drop-down menu list the number of years they have been working with computer security. This was an attempt to see if attitudes would differ with a respondent's level of experience. Lastly, question 5 asked if the respondent is male or female. This question was an attempt to profile the computer security community as well as to see if the two sexes would hold differing attitudes on the full disclosure issue.

Familiarity with Vulnerability Information

Questions 7 and 8 dealt with vulnerability sources used by respondents and their colleagues on a regular basis. This was an attempt to gauge a respondent's familiarity with the different sources of security vulnerability information and to see if there were significant differences in the sources used between the three groups. It was assumed a respondent would be better informed on the full disclosure issue if he/she routinely used a few of the listed sources of vulnerability information. In addition, it was assumed respondents were informed on computer security issues if they knew which vulnerability sources were used by others in their organization. Question 8 was also an attempt to see

if the respondent's job duties do not entail monitoring vulnerability information because someone else in the organization does.

Full Disclosure Arguments

The third section of the survey asked respondents to express their opinions using two different scales. Questions eight and nine used a rating scale of 1-10, with 10 being the strongest set up as follows:

○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6 ○ 7 ○ 8 ○ 9 ○ 10

This rating scale was used because it has been documented useful for purposes of gathering information about a person's perceptions (Thomas 21). In this study, the rating scale provides information about the intensity of a person's feelings towards the effects of fully disclosing vulnerabilities.

Questions ten through twenty used a Likert-type rating scale set up as follows:

○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree

A five-point rating scale presents an interesting predicament for some researchers because it allows a middle answer. Some researchers eliminate the middle answer in a Likert scale to avoid the temptation of respondents to choose a "middle" answer each time (Newton). The elimination of middle answers forces respondents to indicate a positive or negative reaction, in effect taking away their ability to sit on the fence and neither agree or disagree. For purposes of this study, it was believed there could be many

instances in which a person neither agreed nor disagreed with the statement and would thereby select the neutral response. Because full disclosure itself is not a clear issue, respondents were not forced to chose a side.

Focus of Survey

While there are many arguments for and against full disclosure, the survey was limited to include a few issues. This was done to limit the scope of the study and to limit the amount of time it would take a respondent to complete the survey. Therefore, the survey concentrated on selected risks associated with full disclosure, the perceived necessity of the degrees of full disclosure, the argued benefits of full disclosure, and the responsibilities of those who discover vulnerabilities.

Risks

The survey first concentrated on some risks associated with full disclosure, such as the risk the information will aid attackers in carrying out breaches of security. This issue is paramount because without this associated risk, full disclosure would not be as controversial. Furthermore, the risk that full disclosure information will be used for illegal or otherwise dishonest purposes is the primary argument against the full disclosure movement. Question 8 asked respondents to weigh the risk that full disclosure will lead to an increased number of security breaches on the 1-10 rating scale. Evidence exists to prove that the release of full disclosure information may be correlated with an increased number of security breaches (Martin). Therefore, an attempt was made to measure the

tolerance respondents have for living with the risk of an increased number of security breaches.

The risk associated with not following the full disclosure model (also known as "security by obscurity") is addressed in question 9. Question 9 balanced the previous question by asking respondents to evaluate (using the 10 point ranking scale) the danger that may arise from keeping vulnerabilities private. This danger arises from system administrators who are not prepared to defend their systems against vulnerability exploits.

Characteristics that may have some bearing on the level of risk were examined. The level of risk associated with a full disclosure announcement increases when a detailed exploit script to the vulnerability is released. A detailed exploit script then creates more risk if an automated attack tool is written to exploit the vulnerability. Because the aforementioned risk is somewhat commonsensical, the study attempted to examine another characteristic that should have an affect on the level of risk associated with full disclosure.

Question 10 asked respondents their opinions (through use of a 5-point Likert scale) the extent to which they agreed that historical vulnerability information is less risky in the wrong hands compared to recently published vulnerability information. This question was relevant because many with a stake in computer security felt that the time lag in CERT announcements led them to be ineffective, initiating the move to full disclosure mailing lists, such as BugTraq (Schneier 338). On the other hand, many vulnerabilities that have been exploited are those that have been public for sometime and

are published in CERT advisories (Farmer). Therefore, the survey attempted to gather perceptions of which announcements carry the greatest degree of risk for being used in dishonest security efforts, immediate announcements such as those on BugTraq, or more CERT-like announcements, which are those that are kept private for some period of time.

Necessity

Necessity is the quality of being necessary, or absolutely essential. According to dictionary.com, if something is necessary, it is "needed to achieve a certain result or effect." Therefore, the study examined perceptions of how indispensable full disclosure announcements are towards aiding legitimate computer security efforts. Because the level of detail embedded in a full disclosure announcement can effect its usefulness, both towards legitimate computer security efforts and not-so-legitimate efforts, respondents were asked their opinions on the necessity of "full disclosure of vulnerabilities" (question 12) and the necessity of "full disclosure of exploit code" (question 13). Question 12 was written to refer to a definition of full disclosure that does not include the publication of exploit code.

Benefits

Those that defend the full disclosure of computer and network security vulnerabilities may point to many proposed benefits that come from following the full disclosure model. Therefore, perceptions of selected proposed benefits were examined in an effort to gauge whether these benefits do in fact exist and how strongly people believe in them. Question 11 asked respondents (through use of the 5-point Likert scale) their

opinion on whether the "public disclosure of vulnerabilities results in more secure products from vendors." The creation of more secure products is a commonly cited argument in support of the full disclosure movement (Ranum). Furthermore, a counterargument for this proposed benefit has also been widely discussed. Those against full disclosure argue that products are released with security holes based on vulnerabilities commonly known and published (i.e., buffer overruns and invalidated user inputs). Therefore, the counterargument states that full disclosure does not improve the security of products.

Lastly regarding benefits of full disclosure, an attempt was made to examine perceptions of whether certain players in the full disclosure movement are benefited. While it is quite obvious that full disclosure makes life easier for scriptkiddies, the same is not true for whether those employed in computer and network security, vendors, and society as a whole have benefited. Questions 17, 18, and 19 made use of the 5-point Likert scale to ask respondents the extent to which they agreed that full disclosure has benefited the aforementioned parties. The phrase "society as a whole" was meant to include everyday people who depend on computer technology in someway or another. For example, Mr. Joe Average wouldn't benefit from full disclosure if it resulted in unauthorized persons obtaining his social security number. This question regarding the benefits of full disclosure to society also served as an indicator of how strongly a respondent is for or against full disclosure in general.

Responsibilities

The responsibilities of those who discover computer and network security vulnerabilities are often at the forefront of the full disclosure debate. Therefore, the survey contained four questions (using the 5-point Likert scale) about how a person should handle the discovery of a vulnerability. Question 14 asked respondents to state their level of agreement with the following statement, "A security professional has a responsibility to report discovered vulnerabilities to vendors." This question was meant to clarify the responsibilities of the discoverer, regardless of whether the discoverer plans to publicly release the found vulnerability. A strong level of agreement with this statement was expected because both full disclosure opponents and advocates support this protocol of action (the duty to report a bug first to the vendor is stated in the BugTraq FAQs). In order to assess agreement with the BugTraq FAQ response, question 15 asked respondents if a vulnerability should first be reported to the vendor before any such disclosure to the public.

As previously mentioned in Chapter One, Rain Forest Puppy authored a policy on how to handle the discovery of vulnerabilities (FRP). The communications between the discoverer of the vulnerability and the software vendor may be crucial in the timing of a full disclosure announcement. Therefore, question 16 was an attempt to examine how a discoverer should handle an unresponsive vendor. It asked respondents to state their agreement with disclosing a vulnerability if the vendor does not address the vulnerability in a "reasonable amount of time." Because the amount of time needed for a vendor to address a vulnerability may vary depending on the complexity of the bug or the particular

software vendor, question 16 asked respondents to answer the question based on what they would consider a reasonable amount of time.

The full disclosure debate calls for the computer security community to evaluate its ethics. This is in the wake of the so-called greyhat hackers, or legitimately employed security consultants who publish vulnerability announcements and exploit code for purposes of personal financial gain or simply to demonstrate a level of hacking acumen (Ranum's speech). In order to assess perceptions of the ethical climate of the computer security community, question 20 asked respondents if "those employed in computer and network security would benefit from an ethical code of conduct." It was expected that the level of agreement with this statement would be an indicator as to how ethical respondents perceived those working in computer security to be, with a strong level of agreement meaning there is a perceived need for a stronger ethical foundation in the computing security field.

Prior to Survey Distribution

Prior to the study, the research instrument was discussed with a few individuals possessing expertise in computer security. Most notably, a member of the InfraGard Provisional National Executive Board was consulted. In addition, the survey was also reviewed and cleared for content by an FBI InfraGard coordinator. Assurance was given that the survey would not compromise privacy or be used for commercial purposes. In support of this, all contact information for the researcher and project advisor were provided to the FBI. Support from the Columbus, Ohio InfraGard coordinator was as follows:

"While the FBI has not officially partnered with this project, InfraGard is about partnering with the public and private sectors to help bring about a more secure infrastructure. Partnering in this or any such project can help provide all of us insights into the attitudes and behavior of network security personnel. After consultation with Ms. Goens, an examination of her survey, and an assurance that results of this survey will be made available as reference to InfraGard coordinators, hopefully we can make the sampling as complete as possible while demonstrating to others our commitment to obtain objective feedback."

--Columbus InfraGard sub-chapter Coordinator, Cincinnati Division

After attending a meeting of the Columbus, Ohio InfraGard chapter, it was noticeable that InfraGard members as well as the FBI were interested in the survey topic. At the particular meeting attended, an FBI agent presented the latest findings from the annual joint survey of the Computer Security Institute and FBI. Trends concerning security breaches and the limitations of the survey data were discussed. Therefore, those attending InfraGard meetings were perceived as proactive members of the computer security community who would be willing to participate in this study.

CHAPTER 4

RESULTS AND DATA ANALYSIS

Introduction

Survey data was collected through a website, accessed by respondents via a hyperlink embedded in an e-mail message (see Appendix B). Conducting the survey in this manner provided dynamic opportunities to reach a myriad of individuals interested in computer security. Cooperation was gained from several of the FBI-controlled InfraGard chapters and from several of the ISSA chapters. In addition, the survey reached an enormous, global audience with its posting to the BugTraq list. The three samples cannot be considered random samples for purposes of statistical testing. However, the study provoked numerous insightful remarks from participants (see section E, appendix C) and the results present interesting findings on the attitudes of participants in the three computer security groups.

Survey Distribution

Because of the speed of electronic communications, survey respondents were not given as much time to complete the on-line survey as would be given with a paper-based survey. The InfraGard group was approached first on February 14 because cooperation was needed from several FBI special agents. Next, e-mail requests were sent to each of the ISSA chapter presidents on February 28[1]. Because the survey request would directly reach intended participants in the BugTraq group, the e-mail request was posted to the list

[1] An attempt was first made to distribute the survey through contacting the ISSA Board of Directors.

on March 1. All three of the target groups were given a deadline of March 10 to participate in the study.

Complications with Survey Distribution

The electronic format of the survey presented obstacles for some survey participants. However, this was to be expected because design of the survey website was emphasized over functionality in an attempt to gain cooperation from the tightly controlled InfraGard group. For example, the graphical masthead of the academic institution was used to demonstrate the credibility of the researcher. In addition, at the request of the Office of Research Risks Protection for the academic institution, a JavaScript pop-up dialog box was used to audaciously reinforce the idea that users' privacy rights would not be compromised.

The survey was designed in a Microsoft Windows environment and was tested with Microsoft Internet Explorer and Netscape Communicator, two popular web browsers. The survey was inaccessible by those using select other (and in some cases older) technologies. Those using text-only browsers, console e-mail applications, and the Linux operating system, sent e-mail messages noting that they could not access the survey (see section B, Appendix C).

As the result of the use of JavaScript to administer the consent dialog box, complaints were received (See section C, Appendix C). The consent box frustrated UNIX users because it appeared as one long sentence across the computer monitor. However, more prevalent was the paranoia regarding running JavaScript code from an untrusted source. JavaScript has a documented record of opening up security holes (Stein). For example, JavaScript vulnerabilities have allowed such security compromises

as allowing a web page to read and transmit files from an unsuspecting user's machine. Unlike the cgi script used to collect the survey responses, JavaScript code executes on the browser's side of the connection, presenting a security risk to the person attempting to complete the survey.

Most of the e-mail complaints regarding the use of JavaScript were received from BugTraq subscribers. Therefore, the consent dialog box was removed from the BugTraq survey three days after the initial posting in an effort to appease the annoyed survey respondents. The BugTraq JavaScript-free survey was coded with a different hidden variable to separate those respondents from the ones that had to access the JavaScript dialog box. The two BugTraq groups were combined in the analysis of the data.

A few InfraGard and ISSA chapters preferred to announce the survey on their respective websites in addition or in lieu of distribution via e-mail. For example, the San Francisco InfraGard chapter did not feel comfortable forwarding the survey request via e-mail because the chapter receives numerous such requests. Still wishing to be cooperative in the study, a hyperlink to the survey was placed on the San Francisco InfraGard website. A hyperlink to the survey was also placed on the main ISSA international website[2] (see section D, Appendix A). Additionally, the website advertisements limited the ability to trace the number of respondents based on geographic region for the InfraGard and the ISSA groups.[3]

[2] Implications of this are that those not belonging to the target groups may have completed the survey.
[3] For example, the survey hyperlink designated for the ISSA Midwest chapters was placed on the main ISSA international website (www.issa.org). Therefore, it was not surprising that the Midwest ISSA chapters had the greatest number of responses compared to other geographic regions of the ISSA (see table 2).

Responses

Because full disclosure is a fiery, controversial topic in computer security, strong reactions to the study were expected. In addition, a certain amount of reluctance to complete a computer security survey was anticipated. In spite of the sensitivity that exists in regards to computer security topics, an overwhelmingly positive response to the study was achieved. Surprisingly, the "Cancel" button on the JavaScript pop-up dialog box was only clicked twelve times, indicating that individuals were at least willing to view the survey questions before deciding whether to participate. Several of the FBI InfraGard coordinators and the ISSA chapter presidents were very supportive of the study. Some chapters extended invitations for the researcher to attend chapter meetings. In addition, numerous e-mail messages were received from those pleased to see a study regarding the full disclosure issue.

A total of 1425 valid responses and 55 invalid responses were received. For this study, an invalid response is an empty data set that does not contain a hidden variable that identifies to which group a respondent belongs. A user may submit an invalid response by using the browser to directly access the cgi script (in comparison, a valid response is submitted when the click of the "Submit" button calls the cgi script). One may obtain the location of the cgi script (http://fisher.osu.edu/cgi-bin/goens-survey.pl) by viewing the html source code of the survey website. When one directs the browser to http://fisher.osu.edu/cgi-bin/goens-survey.pl, the cgi script is executed without the associated survey responses as intended.

Those who submitted an invalid response might have done so out of curiosity to see what the cgi script would do or out of confusion with the survey process. For example, a BugTraq subscriber sent an e-mail message stating, "There is no indication on the survey page of how to get feedback about the survey, or how one will be able to find the results. I somehow found my way to http://fisher.osu.edu/cgi-bin/goens-counter.pl, which contains your address, without submitting the survey. Otherwise I would not have your address to write." As the contact information for the undergraduate researcher and project advisor were included in the BugTraq e-mail posting, one can only conjecture on other possible areas of confusion that lead to the submission of invalid responses. Additionally, the invalid responses could represent attempts to discredit the survey results.

Responses by Target Group

A different Web URL was distributed to each of the three target groups. In addition, different URLs were distributed within the InfraGard and the ISSA groups. Each Web page included a hidden variable to trace the group to which the respondent belongs. The table below illustrates the number of responses received for each target group[4].

Table 1: Valid survey responses by target group

InfraGard	ISSA	BugTraq
78	61	1266

[4] Out of curiosity or malicious intent, twenty survey respondents found their way to the index web page instead of submitting the survey through the web page given. Because the index URL (http://fisher.osu.edu/people/goens_1) was not directly distributed, the twenty responses received from the index page cannot be traced to the three target groups.

Additionally, the number of responses by geographic regions of the InfraGard and the ISSA chapters are below.

Table 2: Survey responses by geographic region of InfraGard and the ISSA chapters

	InfraGard	ISSA
Northeast	13	4
Midwest	42	27
Southeast	0	5
Southwest	18	13
Westcoast	5	12

Non-response Bias

Because of the limited access to the target groups, it is difficult to meaningfully measure the non-response bias. However, a non-response bias is inherently present. For example, those interested in completing a survey on the topic of full disclosure may have differing attitudes than those not willing to complete the survey. Those that chose not to complete the survey may be more sensitive to security concerns (such as running the JavaScript code), and could potentially represent a different non-response bias. In addition, a number of potential respondents in the target groups were excluded from the survey. For example, some Linux users and those unable to run the JavaScript code sent e-mails stating they would have completed the survey if it were technically feasible for them to do so.

Chi-Square Test of Independence

The chi-square test of independence was used to determine if two variables (the question response and the respondent's group membership) are independent. If the two variables are independent, a respondent's attitudes are not related to the target group in which the respondent belongs. In such a case, the members in the three computer security groups would be expected to hold similar attitudes. The frequencies of responses were tallied into a two-way contingency table. Following is the contingency table for question 8, which asked respondents to rate the risk that full disclosure will lead to an increased number of security breaches.

Table 2: Contingency Table for Question 8

	BugTraq	ISSA	InfraGard	
1	(76.7) 81	(3.7) 2	(4.7) 2	85
2	(79.4) 82	(3.8) 3	(4.8) 3	88
3	(190.3) 196	(9.1) 8	(11.5) 7	211
4	(131.7) 136	(6.3) 7	(8.0) 3	146
5	(149.7) 154	(7.2) 6	(9.1) 6	166
6	(120.0) 119	(5.7) 6	(7.3) 8	133
7	(173.2) 170	(8.3) 10	(10.5) 12	192
8	(179.5) 172	(8.6) 10	(10.9) 17	199
9	(55.9) 48	(2.7) 5	(3.4) 9	62
10	(96.5) 95	(4.6) 3	(5.9) 9	107
	1253	60	76	1389

The numbers in parentheses represent the expected, or theoretical frequencies, which can be determined by

Formula 1:

$$e_{ij} = \frac{(n_i)(n_j)}{N}$$

Where:
i is the row
j is the column
n_i is the total of row i
n_j is the total of column j, and
N is the total of all frequencies (Black 825).

Using these expected and observed frequency values, the chi-square test (χ^2) of independence can be computed to determine whether the variables are independent. The null hypothesis is that the two variables are independent. The statistical test is

Formula 2:

$$\chi^2 = \sum\sum \frac{(f_o - f_e)^2}{f_e}$$

where:
degrees of freedom = (number of rows-1)(number of columns-1)
f_o = observed value
f_e = expected value.

After choosing an alpha level, one can use the degrees of freedom to find the critical value of chi-square from a statistical table reference. Using the above example, the critical value of chi-square for $\alpha = .01$ is $\chi^2_{.01, 18} = 34.8053$ (Black A-26). The decision rule is to reject the null hypothesis if the observed chi-square (χ^2 value) is greater than 34.8053. The chi-square value computed from Table 2 (using Formula 2) is 29.414, meaning the null hypothesis cannot be rejected. The acceptance of the null hypothesis means the attitudes of the respondents are independent of the group to which they belong. However, in regards to question 8, the statistical test presents limitations and any conclusions drawn from its application are suspect.

A problem arises because of the small-expected frequency values in some of the ISSA and InfraGard cells. Contingency tables should not be used with a great number of expected cell values of less than 5 because the small-expected frequencies can lead to inordinately large chi-square values (829). Therefore, for the analysis of questions 8 and 9, the 1-10 rating scale to a 1-5 scale was collapsed to avoid the small expected values. The recoding scheme to collapse the data is as follows:

Table 3: Recoding of 1-10 Rating Scale to 1-5 Rating Scale

Old Value	New Value
1, 2	1
3, 4	2
5, 6	3
7, 8	4
9, 10	5

A new contingency table for question 8 follows:

Table 4: Collapsed Contingency Table for Question 8

	BugTraq	ISSA	InfraGard	
1	(156.06) 163	(7.47) 5	(9.47) 5	173
2	(322.05) 332	(15.42) 15	(19.53) 10	357
3	(269.72) 273	(12.92) 12	(16.36) 14	299
4	(352.72) 342	(16.89) 20	(21.4) 29	391
5	(152.45) 143	(7.3) 8	(9.25) 18	169
	1253	60	76	1389

Running the chi-square test with the collapsed categories reduces the degrees of freedom to 8. The critical value for $\chi^2_{.01,8}$ is 20.0902 (Black A-26). Using Formula 2 with the collapsed contingency table yields a chi-square value of 21.1176, which is greater than the critical value. Therefore, collapsing the ranking categories leads to the rejection of the null hypothesis. Because there are no problems with small-expected

frequencies in the collapsed test, one can conclude that perceptions of the risk associated with full disclosure is dependent on association with the computer security groups.

P-Value

The P-value method tests the probability of getting a test statistic at least as extreme as the observed test statistic under the assumption that the null hypothesis is true. The p-value represents the smallest value of alpha for which the null hypothesis can be rejected (Black 367). For example, if the p-value of a test is .05, the null hypothesis cannot be rejected at $\alpha = .01$ because .05 is the smallest value of alpha for which the null hypothesis can be rejected. Therefore, the null hypothesis can be rejected at significance levels > .05. In this study, a statistical computer program yielded p-values using the chi-square test of independence. P-values were computed for questions 8-20 and are presented in Table 5 below[5].

Table 5: Computed p-values

Question	8	9	10	11	12	13	14	15	16	17	18	19	20
p-value	.0067	.0197	.2562	<.0001	<.0001	.0339	.2902	.7324	<.0001	<.0001	.0002	<.0001	0.0288

[5] The computer statistics package marked the chi-squares as suspect in questions 11, 12, and 14-20 due to expected frequency counts less than 5. However, the statistical test is not severely limited in these cases. Collapsing the 1-5 ranking scales further would still lead to small-expected frequencies in the InfraGard and the ISSA samples. Additionally, as the p-values are extremely small, more confidence may be placed in the accuracy of the statistical test.

Results

Background of Survey Respondents

Simple summary statistics were complied for questions 1-7, which shed light on the background of survey respondents. The results for questions 1-7 may be found in Appendix D. 1311 respondents answered the first question; with 96% of them answering that they are responsible for computer or network security in some way. The questionnaire was not comprehensive in listing the common job titles of the survey respondents as 20% of the respondents that answered the question chose the "other" response. A general trend was noted that members of the ISSA and InfraGard were more likely to be employed in IS management and consulting positions than those belonging to the BugTraq group.

Question 3 asks what primary industry the respondent is employed. Evidently, the drop down menu of options was not comprehensive enough because the highest percentage of respondents chose the "other" response. Regardless, some trends were noted that correlate with the previous question. For example, the ISSA respondents have the highest percentage of those with consulting job titles and the highest percentage of those employed in the consulting services industry. Examination of the responses from question 3 shows that the health care and utilities industries are not as heavily represented in the BugTraq group. In addition, as might be expected from InfraGard's foundation with the FBI, InfraGard respondents have the highest percentage (21.05%) of those employed by the government.

Most of the survey respondents (75.5%) have five years or less of experience working with computer security. However, there are noticeable differences in the experience level by target group. Over half of both the ISSA and InfraGard respondents have greater than 5 years of experience, as compared to 21.5% of the BugTraq respondents. Most BugTraq respondents (62.78%) fall into a computer security experience level of 2-5 years.

Males heavily dominate the computer security field, as corroborated by the survey results. 96% of the survey respondents are male. Interestingly, there were a much higher percentage of female respondents in the ISSA and InfraGard groups. InfraGard and the ISSA respondents are 15.79% and 11.67% female, as compared with 2.91% in the BugTraq group.

Questions 6 and 7 inquire on what sources of computer security vulnerability information the respondent and respondent's colleagues regularly monitor. Securityfocus.com, the organization currently hosting the BugTraq mailing list, is regularly monitored by 69.6% of the survey respondents. As to be expected, 93% of survey respondents use the securityfocus.com mailing lists, such as BugTraq[6]. The "other mailing lists or newsgroup" option was chosen by 53.7% of survey respondents. Survey respondents were less familiar with vulnerability information provided by government agencies and academic institutions. However, a relatively high percentage of survey respondents (66%) said that they regularly monitor information from CERT (previously discussed in chapter 1). Exactly half of survey respondents regularly monitor

[6] The "NT BugTraq" mailing list was mistakenly included in the description for the securityfocus.com mailing lists. The NT BugTraq mailing list is hosted by ntbugtraq.com. Two e-mails were received from survey respondents commenting on this error.

vendor websites for computer security information. Over half (59.7%) visit hacker websites[7]. The frequencies for question 7, which asked respondents about the sources their colleagues use, were similar to the question 6 results.

The Risks of Full Disclosure

As supported by the p-values in Table 5, the null hypothesis that perceptions of risk are independent of the respondent's group membership can be rejected for questions 8 and 9. In other words, perceptions of full disclosure vary depending on what computer security groups with which a person is associated. There are significant differences to how those in BugTraq rated the full disclosure risks compared to those in the more controlled groups. For example, BugTraq respondents did not place a high weight on the risk that full disclosure will lead to an increased number of security breaches. Not surprisingly, those in InfraGard rated the risk of an increased number of security breaches the highest. In regards to the risk of not disclosing a vulnerability, the differences among the three groups are not as pronounced, although the p-value indicates the groups are still significantly different. BugTraq and the ISSA respondents placed a higher rate on the risk of not disclosing a vulnerability when compared to the InfraGard respondents.

There was no significant difference among the target groups for question 10, which asked about risk in relation to the timing of vulnerability information. Overall, respondents did not feel strongly that historical vulnerability information is less risky in

[7] The researcher's intention was for the term "hacker websites" to include such infamous groups as Phrack Magazine (www.phrack.com) and The Cult of the Dead Cow (www.cultdeadcow.com). However, as the term "hacker" may include both black hat and white hat hackers, survey respondents may have included such sites as www.hackers.com, which pledges to uphold the traditional role of hacking as a curious, but not malicious or destructive activity. One e-mail message was received from a survey respondent commenting on the broadness of the term "hacker."

the wrong hands. In other words, survey respondents would agree that attackers are able to compromise systems using vulnerabilities that have been public for quite some time. However, a high level of agreement or disagreement with the statement was not achieved. Therefore, it is hard to draw conclusions on how those in the computer security community perceive the risk associated with the timing of vulnerability information.

Some confusion existed in regards to the wording of questions 8, 9, and 10. Several e-mail messages were received from survey respondents who were unable to interpret what specifically the questions were asking (see Appendix C, section D). The confusion may have caused survey respondents to not answer the questions. Additionally, confused respondents may have been prompted to choose the neutral response.

Necessity of Full Disclosure

BugTraq subscribers feel stronger that full disclosure is necessary for legitimate security purposes. However, most ISSA and InfraGard respondents agreed or strongly agreed with the statement "Full disclosure of vulnerabilities is necessary for legitimate security purposes." Question 13, which asks if "full disclosure of exploit code is necessary for legitimate security purposes," was an attempt to gauge how attitudes would change from the previous question when exploit code is involved. The null hypothesis that attitudes are independent of group membership cannot be rejected at alpha levels of .01, but may be rejected at alpha levels > .0339. Regardless, there is a high level of support for the disclosure of exploit code from the different computer security groups.

56.98% of BugTraq respondents agreed or strongly agreed with the statement, while ISSA and InfraGard had 45% and 46.06% agreement.

Benefits of Full Disclosure

The majority of respondents indicated that they perceive the argued benefits of full disclosure to exist. A higher percentage of BugTraq subscribers (90.82%) felt that full disclosure results in more secure products from vendors. However, the more controlled groups also indicated a high level of agreement with the idea that full disclosure results in more secure products. 85% of the ISSA and 75% of InfraGard respondents agreed or strongly agreed with more secure products being produced.

When asked if those employed in computer security have benefited from full disclosure (question 17), the overwhelming majorities in all three groups indicate that the computer security community has benefited. A lesser majority indicated that vendors have benefited from full disclosure. The ISSA respondents indicated a lower level of agreement with vendor benefits, as 28.33% of group respondents chose the neutral response. Not surprisingly, the all-encompassing statement, "Society as a whole has benefited from full disclosure," received a majority of agreement from respondents. The low p-values for the questions regarding benefits indicate the attitudes are not independent of group membership.

Responsibilities

Respondents in the three groups share similar attitudes on the responsibilities of those working in computer security. The majority agreed with the statement, "A security

professional has the responsibility to report discovered vulnerabilities to vendors." Interestingly enough, no one in the ISSA group disagreed with this statement, while three respondents in the InfraGard group disagreed. The majorities also indicate that vulnerabilities should be reported to the vendor prior to disclosing the vulnerability to the public. Again, nobody in the ISSA group disagreed with first reporting a vulnerability to the vendor, while one respondent from InfraGard disagreed. The three groups differed more in response to the statement, "Assuming a vulnerability is reported to a vendor, if that vendor does not address the reported vulnerability in what you consider a reasonable amount of time, that vulnerability should be made public" (question 16). As would be expected, the BugTraq group held the highest level of agreement with the previous statement. However, the majorities (79.66% and 80.27%) in the ISSA and InfraGard also agreed with the statement, supporting full disclosure announcements in the absence of vendor cooperation.

The majorities in all three groups agreed that those working in computer security would benefit from an ethical code of conduct. As the ISSA and InfraGard groups have an established ethical code for members, one would expect these two groups to hold the highest level of support for a code of conduct. While the ISSA and InfraGard groups did have a high level of agreement with a code of conduct, 75% of the BugTraq respondents agreed that the computer security community would benefit from an ethical code.

CHAPTER 5

CONCLUSION

Summary

The goal of this study was to determine how the computer security community perceives the proposed benefits and trade-offs of risk associated with full disclosure. Additionally, attitudes concerning the responsibilities of those who discover computer security vulnerabilities were examined. Three groups of those interested in computer security were surveyed and results were compared across groups.

The majority of participants in the study were subscribers to the BugTraq full disclosure mailing list. Participation was gained from several chapters of the FBI-coordinated computer security group, InfraGard. Additionally, several chapters of the Information Systems Security Association (ISSA), a professional membership organization, participated in the study. Conclusions drawn from the results follow below.

Conclusions

Survey data yielded several interesting findings that are discussed below.

1. Perceptions of the degree of risk involved with full disclosure announcements vary depending on a person's association in certain computer security groups. BugTraq subscribers do not feel full disclosure is as harmful as those in professional membership computer security groups, such as the ISSA. Not surprisingly, BugTraq subscribers feel the strongest that *not* releasing vulnerability information will cause a high degree of risk for those involved with computer security. These results show that there is no strong consensus regarding

the possible effects of full disclosure across the various types of persons employed in computer security.

2. There is a high level of perceived necessity for full disclosure announcements in aiding legitimate security efforts. Attitudes regarding the necessity of full disclosure are not independent on association in various computer security groups. However, attitudes explicitly regarding the necessity of exploit code are similar across groups.
3. Agreement on a broad range of ideas concerning perceived benefits of full disclosure is not independent of group membership. For example, BugTraq subscribers felt the strongest that full disclosure does result in more secure products.
4. Attitudes on reporting vulnerabilities to vendors are independent of group membership. There was a consensus that those working in computer security should report discovered vulnerabilities to the vendors of the vulnerable products. Consensus was remarkably strong that vulnerabilities should be reported first to the vendor before disclosure to the public.
5. Opinions about whether vulnerabilities should be publicly disclosed in the absence of vendor cooperation are not independent of group membership. Consistent with the mindset of the previous findings, BugTraq subscribers felt the strongest that vulnerabilities need to be publicly disclosed if the vendor does not address the reported vulnerability in a reasonable amount of time.
6. The outlook on whether those employed in computer and network security would benefit from an ethical code of conduct is independent of group membership.

Respondents across the three types of groups surveyed felt a code of ethical would be beneficial.

Limitations

Limitations in this study arise from problems in the technical format of the on-line survey, the method in which the survey was distributed, and from the wording of the survey questions. The study failed to survey a representative sample of those in the computer security community due to the exclusion of Linux users and those unable or unwilling to run the JavaScript code. Survey distribution was difficult to control. The number of persons receiving the survey e-mail request could not be controlled in the instance of the InfraGard and the ISSA groups. Those outside of the three target groups could have access to the survey. Additionally, no mechanisms were put into place to prevent respondents from submitting the survey more than once. It was believed that if such mechanisms were utilized, such as collecting the e-mail addresses of respondents, it would discourage participation and perhaps serve as a challenge for some to find ways around the survey controls.

The study demonstrates the importance of carefully wording survey questions. From the numerous e-mails sent regarding the wording of questions, it must be noted that the wording used presents limitations to the study. Several respondents were confused as to what the questions were asking and would have liked additional clarification (see section D, Appendix C). Responses to the questions may vary depending on how a person interpreted what the question was asking.

Recommendations for Future Research

This study supports the idea that those in the computer security community generally favor the full disclosure model of disseminating vulnerability information. This raises important questions, as full disclosure is not a clear issue. The severity of the vulnerability involved, the specific vendor involved, and the number of vulnerable systems in the wild plays an important role on the good/harm that full disclosure brings. Therefore, examination of attitudes regarding several scenarios of vulnerabilities may bring additional clarification to how those in the computer security community would prefer vulnerability information to be handled.

This study shows that a strong majority supports contacting vendors with security vulnerabilities before releasing the information to the public. Therefore, research on *how* vulnerabilities should be disclosed would be beneficial to the current body of knowledge. Rain Forest Puppy's Full Disclosure Policy v2.0 provides a start in this direction. However, the policy itself could be tested for its influence and usefulness.

Specific to this study, survey data may be examined more in depth to examine if the background of survey respondents has a significant relationship on their attitudes regarding full disclosure. For example, significances may be uncovered across experience levels or industry sectors. While such findings may be considered anecdotal, they may provide future direction for those wishing to study social and ethical issues in computing.

BIBLIOGRAPHY

Black, Ken. Business Statistics, Contemporary Decision Making. Minneapolis/St.Paul: West Publishing Company, 1997.

CERT. "The CERT Coordination Center Vulnerability Disclosure Policy." http://www.cert.org/faq/vuldisclosurepolicy.html (18 April 2001).

---. "Welcome to the CERT/CC Vulnerability Notes Database!" http://www.kb.cert.org/vuls/ (18 April 2001).

Computer Security Institute. "2000 CSI/FBI Computer Crime and Security Survey," Computer Security Issues & Trends. Vol. VI. No 1, Spring 2000.

Dictionary.com. On-line search for: "necessary." http://www.dictionary.com/cgi-bin/dict.pl?term=necessary (5 April 2001).

Farmer, Dan. "Shall We Dust Moscow?" December 18, 1996, http://www.fish.com/survey. (20 March 2001).

FBI. "National Press Office Immediate Release." January 5, 2001, http://www.infragard.net/national_rollout/pressrelease.html (31 March 2001).

Greenstein, Marilyn, ed. Security, Risk Management and Control. By Todd Feinman. Boston: McGraw Hill, 1999.

InfraGard. "InfraGard National By-Laws, Code of Ethics, and Membership Application." http://www.columbus.oh.us/infragard/ (31 March 2001).

Internet Indicators. "Facts & Figures." http://www.internetindicators.com/facts.html (22 April 2001).

ISSA. "Information Systems Security Association." http://www.issa.org/ (1 April 2001).

---. "ISSA Signup page." https://www.issa.org/signupform.taf (1 April 2001).

---. "Code of Ethics." http://www.issa.org/codeofethics.html (1 April 2001).

Koch, Lewis Z. "Ranum in the Lion's Den." ZDNet. Sept. 21, 2000. http://www.zdnet.com/intweek/stories/columns/0,4164,2630983,00.html (1 November 2000).

Kurtz, George, McClure, Stuart, Scambray, Joel. Hacking Exposed: Network Security Secrets and Solutions. Berkeley: Osborne/McGraw-Hill, 2001.

Martin, Brian. "A note on security disclosures." ;login:, Vol 25 No 8. Dec. 2000: 43-46.

McClure, Stuart. "Anti-hacking method of full disclosure under attack from a part of the security industry." InfoWorld.com. Aug 11, 2000, http://www2.infoworld.com/articles/op/xml/00/08/14/000814opswatch.xml?Template=/storypages/printarticle.html (11 February 2001).

McGraw, Gary and Viega, John. "Make your software behave: Learning the basics of buffer overflows." IBM developerWorks. March 1, 2000. http://www-106.ibm.com/developerworks/library/overflows/ (12 April 2001).

Newton, Robert, et al. "Development and Evaluation of WWW Resources to Support Research Methods and Electronic Engineering: a comparison," http://www.marble.ac.uk/ltdi/evalstudies/eswwwres.htm (5 April 2001).

Pond, Weld. "Do security holes demand full disclosure?." ZDNet. Aug 16, 2000, http://www.zdnet.com/zdnn/stories/comment/0,5859,2615973,00.html (2 February 2001).

Rain Forest Puppy. "Full Disclosure Policy v.2.0." http://www.wiretrip.net/rfp/policy.html (2 November 2000).

Ranum, Marcus. "Have a Cocktail: Computer Security Today." http://web.ranum.com/usenix/ranum_elx_cocktail.pdf (20 April 2001).

---. "Script Kiddiez Suck." Black Hat Briefings 2000. Las Vegas, 26 July 2000.

---. "The Network Police Blotter: Buffer Overruns and burglar alarms." http://web.ranum.com/usenix/ranum_2.pdf (20 April 2001).

---. "The Network Police Blotter: Full Disclosure is bogus." http://web.ranum.com/usenix/ranum_5_temp.pdf (20 April 2001).

Rauch, Jeremy. "The Future of Vulnerability Disclosure?" ;login:. http://www.usenix.org/publications/login/1999-11/features/disclosure.html (1 January 2001).

Rodger, Will. "The FBI's InfraGard Project." ZDNet. Oct. 5, 1998, http://www.zdnet.com/intweek/stories/news/0,4164,357866,00.html (10 October 2000).

San Francisco InfraGard. "Origins of InfraGard." http://www.fbi.gov/contact/fo/sl/origins.htm (31 March 2001).

Securityfocus.com. "BugTraq FAQs." http://www.securityfocus.com/frames/?content=/forums/bugtraq/faq.html (1 March 2001).

Schneier, Bruce. "Full Disclosure and the Window of Exposure." Crypto-Gram. September 15, 2000, http://www.counterpane.com/crypto-gram-0009.html (6 February 2001).

---. "Full Disclosure and Lockmaking." Crypto-Gram. July 15, 2000. http://www.counterpane.com/crypto-gram-0007.html (6 February 2001).

---. Secrets & Lies, Digital Security in a Networked World. New York: John Wiley & Sons, Inc, 2000.

Schweitzer, James A. Protecting Business Information: A Manager's Guide. Boston: Butterworth-Heinemann, 1996.

Spanbauer, Scott. "IE5 Bug-Free? Don't Believe It." PCWorld.com. April 20, 1999, http://www.pcworld.com/resource/article/0,aid,10579,00.asp (22 April 2001).

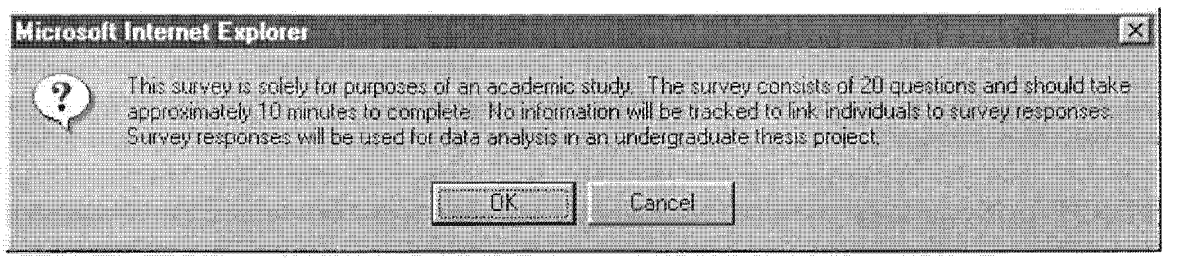
Stein, Lincoln. "The World Wide Web Security FAQ." World Wide Web Consortium. April 2, 2000, http://www.w3.org/Security/Faq/wwwsf7.html (26 April 2001).

The Clinton Administration. "Policy on Critical Infrastructure Protection: Presidential Decision Directive 63." May 22, 1998, http://www.fas.org/irp/offdocs/paper598.htm (31 March 2001).

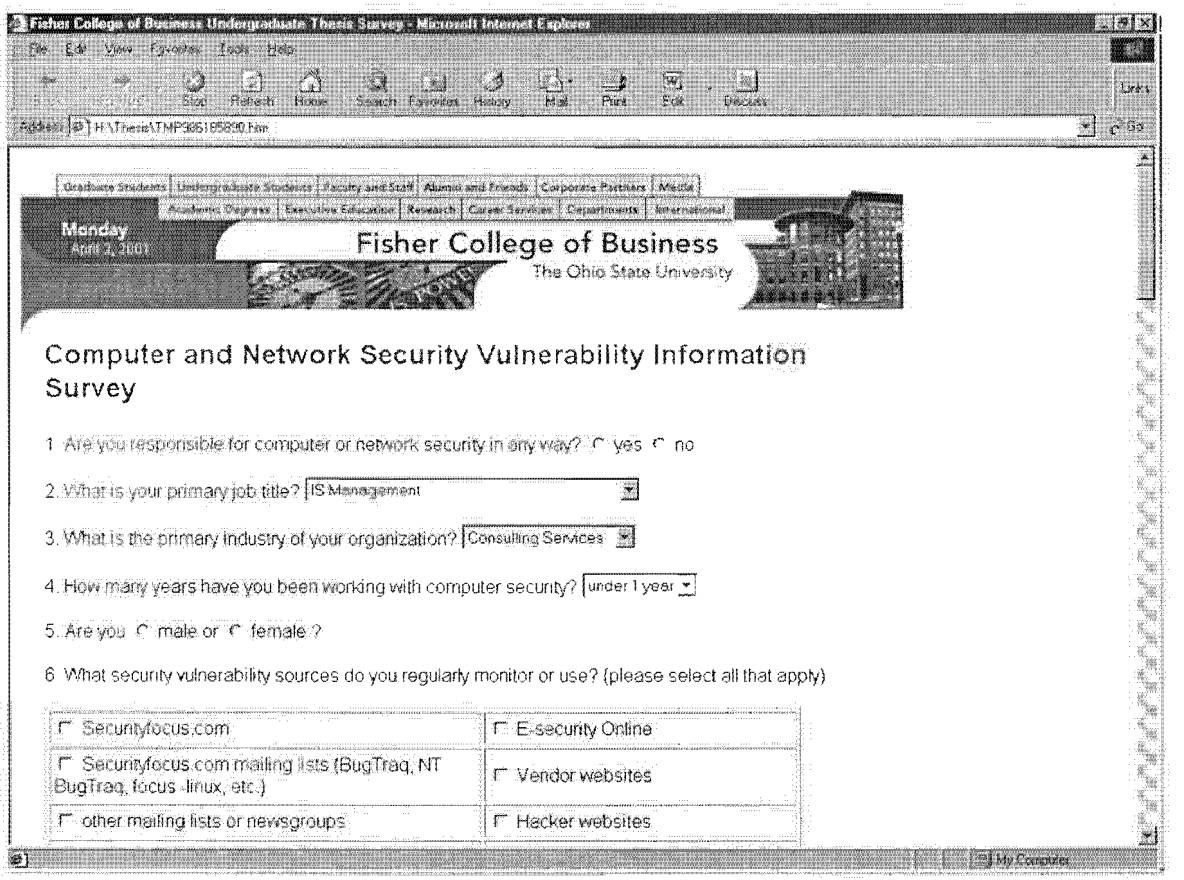
Thomas, Susan J. Designing Surveys That Work: A Step-by-Step Guide. Thousand Oaks: Corwin Press, 1999.

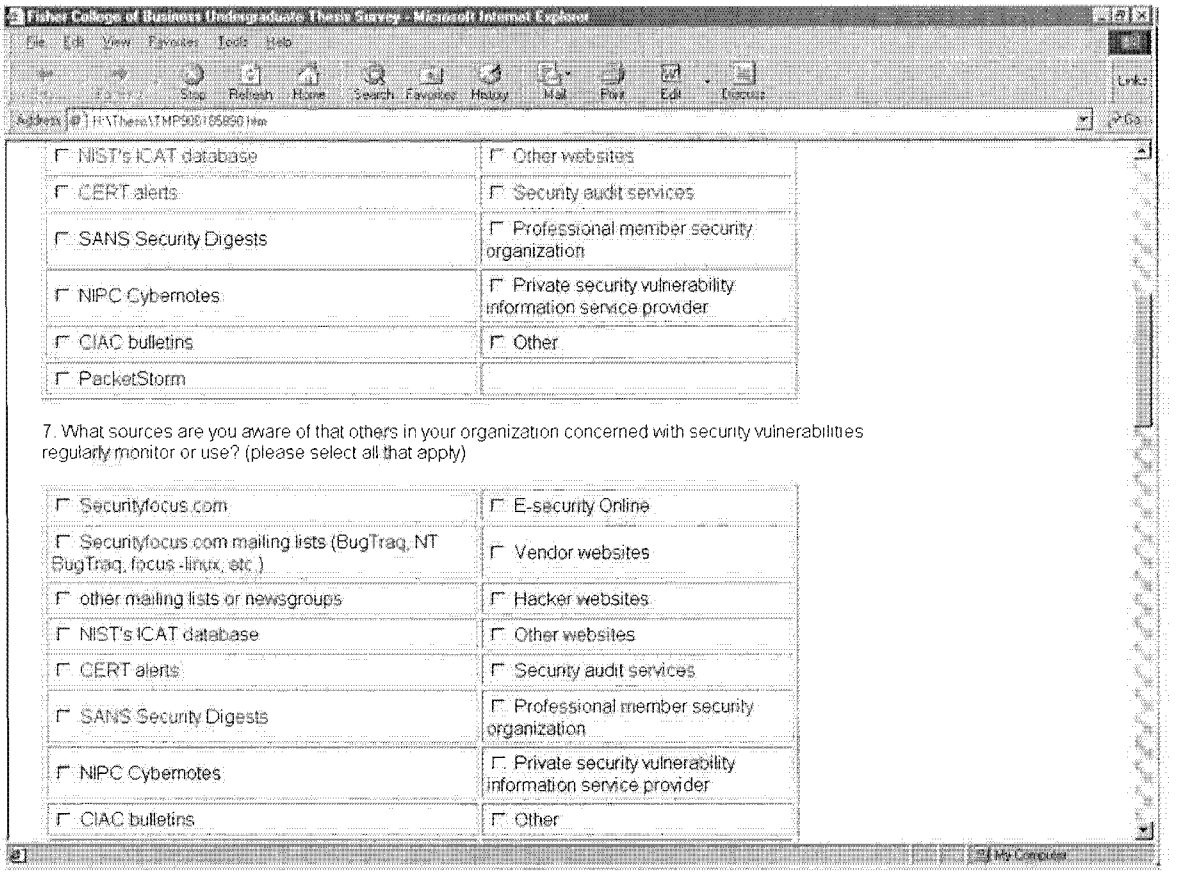
APPENDIX A

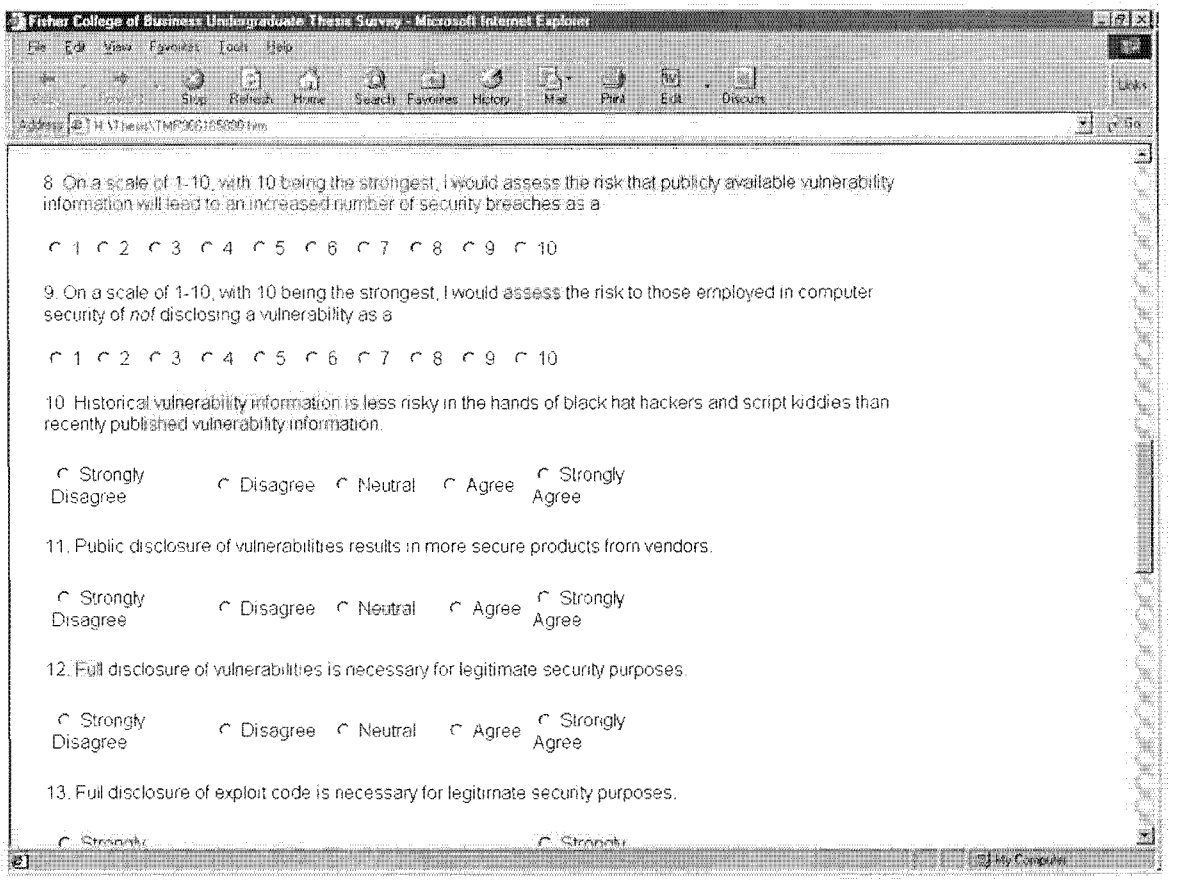
A. A potential survey respondent is first taken to the below dialog box to confirm agreement with the survey terms.

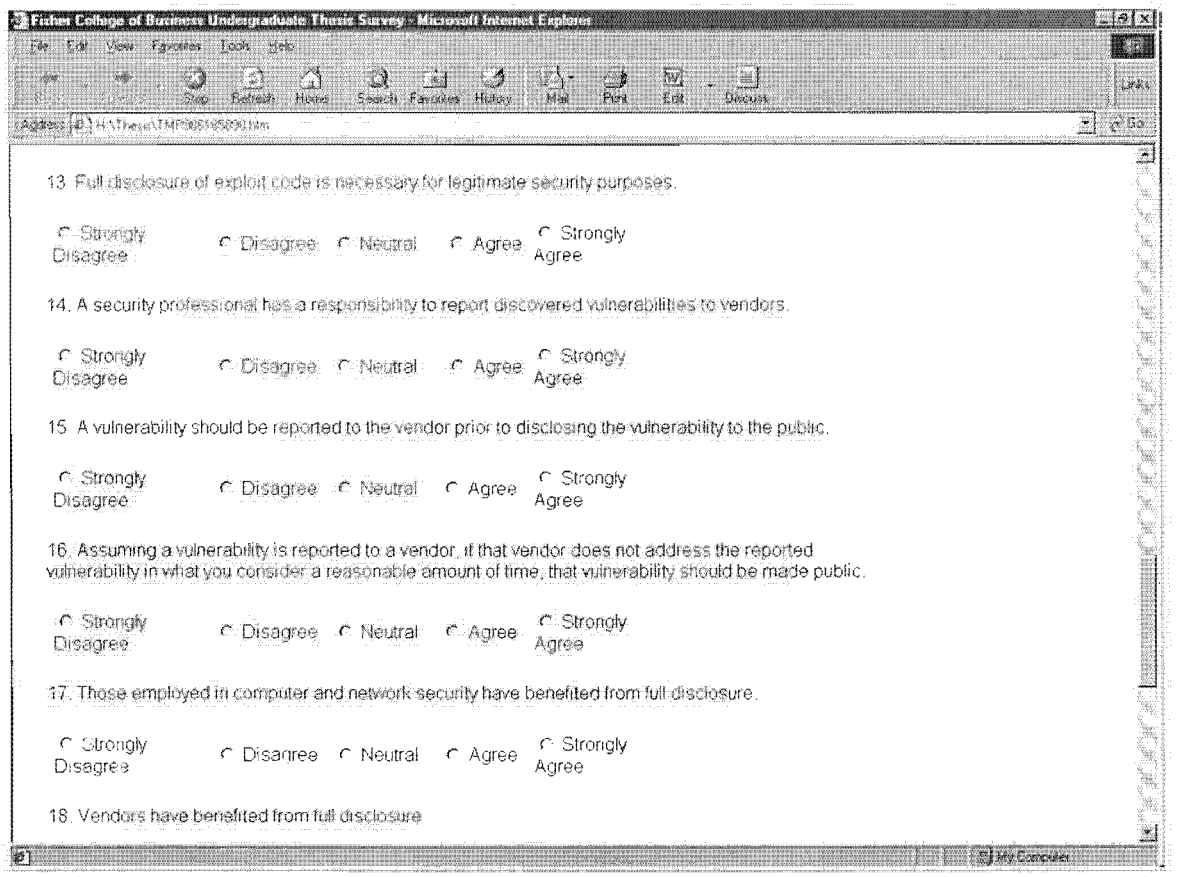


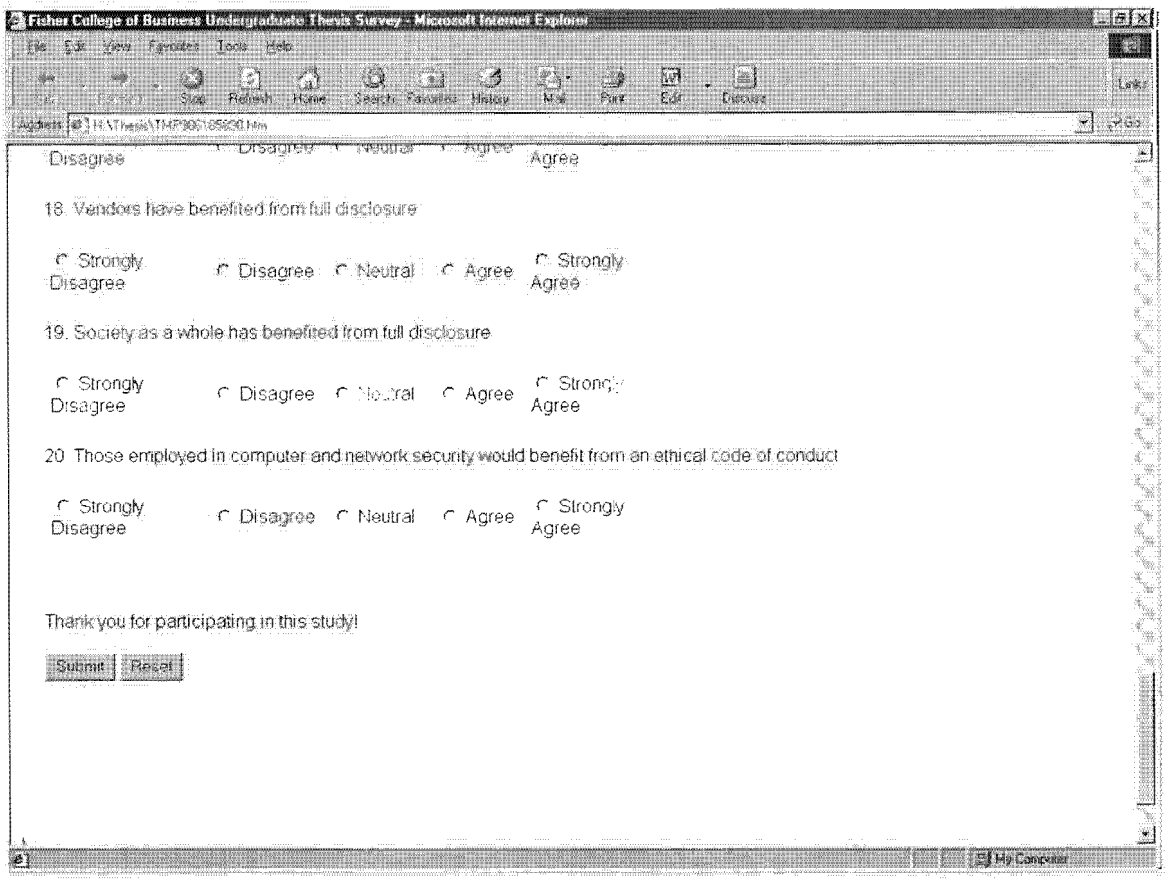
B. After a potential respondent clicks "OK" in the above dialog box, the twenty-question survey is displayed in the potential respondent's web browser.



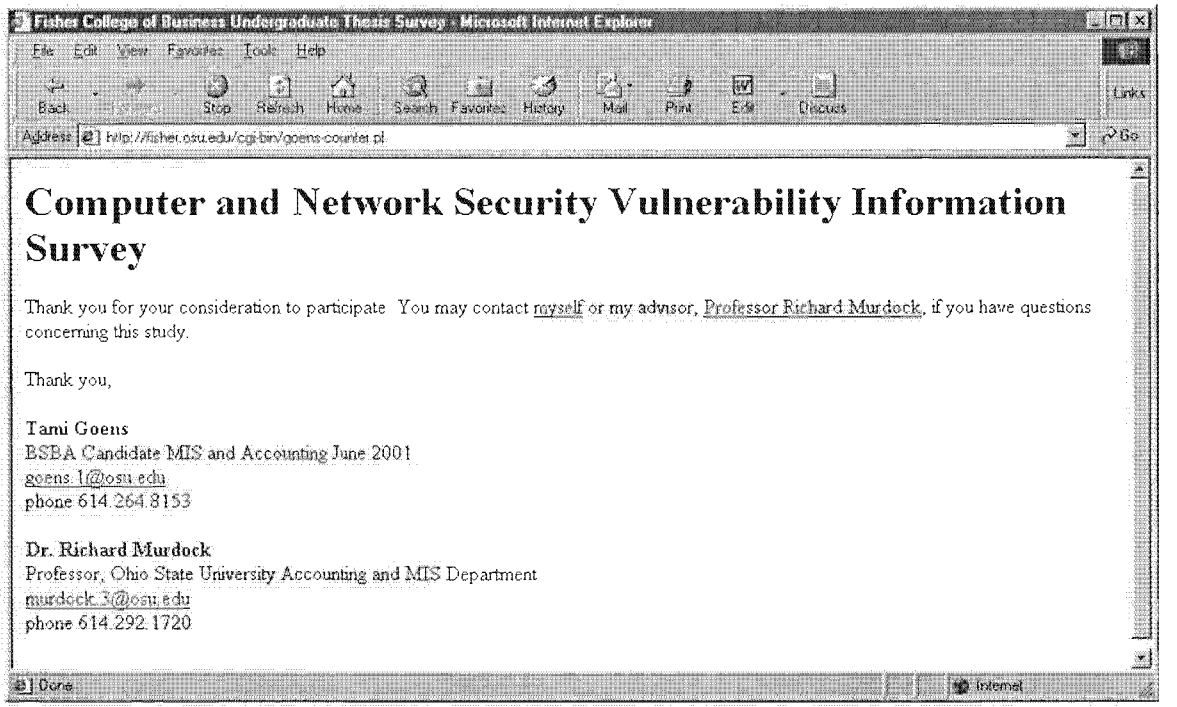

Fisher College of Business Undergraduate Thesis Survey - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Stop Refresh Home Search Favorites History Mail Print Edit Discuss
Address H:\Thesis\TMP90185890.htm
NIST's ICAT database
CERT alerts
SANS Security Digests
NIPC Cybernotes
CIAC bulletins
PacketStorm
Other websites
Security audit services
Professional member security organization
Private security vulnerability information service provider
Other
7. What sources are you aware of that others in your organization concerned with security vulnerabilities regularly monitor or use? (please select all that apply)
Securityfocus.com
Securityfocus.com mailing lists (BugTraq, NT BugTraq, focus-linux, etc.)
other mailing lists or newsgroups
NIST's ICAT database
CERT alerts
SANS Security Digests
NIPC Cybernotes
CIAC bulletins
E-security Online
Vendor websites
Hacker websites
Other websites
Security audit services
Professional member security organization
Private security vulnerability information service provider
Other
My Computer


Fisher College of Business Undergraduate Thesis Survey - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Stop Refresh Home Search Favorites History Mail Print Edit Discuss
Links
Address H:\Thesis\TMP[illegible].htm
Go
8. On a scale of 1-10, with 10 being the strongest, I would assess the risk that publicly available vulnerability information will lead to an increased number of security breaches as a
1 2 3 4 5 6 7 8 9 10
9. On a scale of 1-10, with 10 being the strongest, I would assess the risk to those employed in computer security of *not* disclosing a vulnerability as a
1 2 3 4 5 6 7 8 9 10
10. Historical vulnerability information is less risky in the hands of black hat hackers and script kiddies than recently published vulnerability information.
Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree
11. Public disclosure of vulnerabilities results in more secure products from vendors.
Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree
12. Full disclosure of vulnerabilities is necessary for legitimate security purposes.
Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree
13. Full disclosure of exploit code is necessary for legitimate security purposes.
My Computer

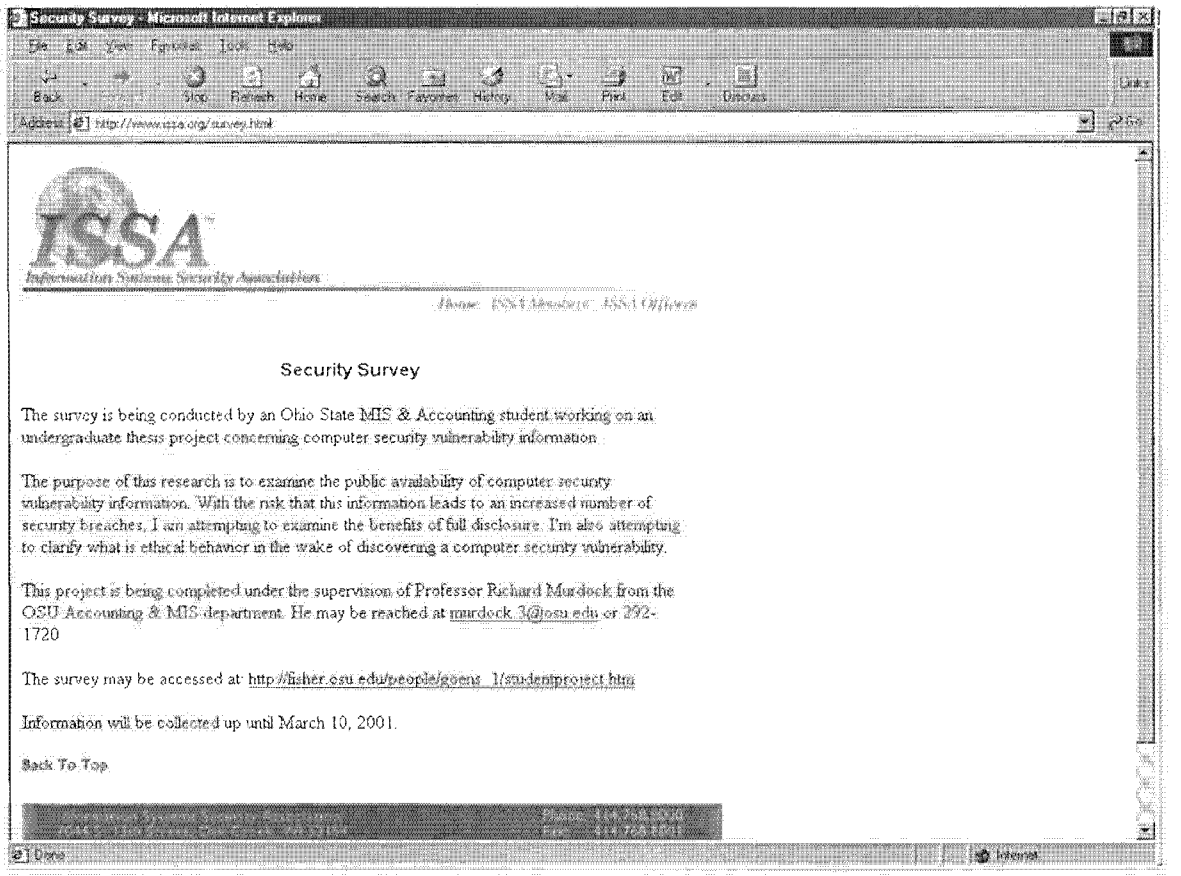

Fisher College of Business Undergraduate Thesis Survey - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Stop Refresh Home Search Favorites History Mail Print Edit Discuss
Address H:\Thesis\TMP9081958901.htm
13. Full disclosure of exploit code is necessary for legitimate security purposes.
Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree
14. A security professional has a responsibility to report discovered vulnerabilities to vendors.
Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree
15. A vulnerability should be reported to the vendor prior to disclosing the vulnerability to the public.
Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree
16. Assuming a vulnerability is reported to a vendor, if that vendor does not address the reported vulnerability in what you consider a reasonable amount of time, that vulnerability should be made public.
Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree
17. Those employed in computer and network security have benefited from full disclosure.
Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree
18. Vendors have benefited from full disclosure
My Computer


Fisher College of Business Undergraduate Thesis Survey - Microsoft Internet Explorer
Disagree
Agree
18. Vendors have benefited from full disclosure
Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree
19. Society as a whole has benefited from full disclosure
Strongly Disagree
Disagree
Agree
Strongly Agree
20. Those employed in computer and network security would benefit from an ethical code of conduct
Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree
Thank you for participating in this study!
Submit
Reset

C. If a potential respondent does not agree to the terms of the survey, the below screen will be displayed in the potential respondent's web browser.



D. A few of the InfraGard and the ISSA chapters advertised the survey on their respective websites. Below is a description of the study found on the International website for the ISSA.



APPENDIX B

A. Below is the message sent to BugTraq subscribers.

BUGTRAQ subscribers,
I'm an Ohio State University MIS & Accounting student working on an undergraduate thesis project concerning computer security vulnerability information. I have developed a questionnaire on the topic of full disclosure. I would appreciate your taking ten minutes or so to complete the survey below:
http://fisher.osu.edu/people/goens_1/fulldisclosuresurvey.htm

I will be collecting survey responses up until March 10, 2001. I will not be tracking IP addresses or linking survey responses to individuals in any way. I would be more than happy to share the results of this survey when my project is complete.

The results of this survey will be used to support my undergraduate thesis project so I may graduate "with distinction" in MIS. I am completing this project under the supervision of Professor Richard Murdock from the OSU Accounting & MIS department. He may be reached at murdock.3@osu.edu or 292-1720.

Sincerely,
Tami Goens
BSBA MIS & Accounting 6/01
The Ohio State University
goens.1@osu.edu
home 614.421.0318
cell 614.264.8153

Dr. Richard Murdock
Thesis Advisor
Professor, Ohio State University
Accounting & MIS Department
murdock.3@osu.edu
office 614.292.1720

B. Below is the message sent to InfraGard coordinators.

Mr./Ms. <<InfraGard Coordinator>>,
I am a student from The Ohio State University completing a thesis project on the full disclosure of security vulnerability information. I understand that InfraGard does not disseminate the e-mail addresses of members. Therefore, I'm asking that you please forward my survey instead of directly providing me with member addresses. Support from the local Columbus, OH chapter is as follows:

"While the FBI has not officially partnered with this project, InfraGard is about partnering with the public and private sectors to help bring about a more secure infrastructure. Partnering in this or any such project can help provide all of us insights into the attitudes and behavior of network security personnel. After consultation with Ms. Goens, an examination of her survey, and an assurance that results of this survey will be made available as reference to InfraGard coordinators, hopefully we can make the sampling as complete as possible while demonstrating to others our commitment to obtain objective feedback."
--Columbus InfraGard sub-chapter Coordinator, Cincinnati Division

Below is a link to my survey on the full disclosure of security vulnerability information. I will be collecting survey responses up until March 10, 2001. I appreciate your cooperation in forwarding this link to your chapter members.

http://fisher.osu.edu/people/goens_1/studentsurvey.htm

This survey is for my undergraduate thesis distinction project at The Ohio State University. To alleviate privacy concerns, I will not be tracking IP addresses or linking survey responses to individuals. I am attempting to distribute my survey to every chapter of InfraGard nationwide. I will be certain to share the results of this survey with InfraGard.

I am completing this project under the supervision of Professor Richard Murdock. Please feel free to contact my advisor or me if there are any remaining questions.

Sincerely,
Tami Goens
BSBA Candidate MIS & Accounting
The Ohio State University
Goens.1@osu.edu
Home 614.421.0318
Cell 614.264.8153

Thesis Advisor
Dr. Richard Murdock
Professor, Accounting & MIS Dept
The Ohio State University
Murdock.3@osu.edu
Office 614.292.1720

C. Below is the message sent to the ISSA chapter presidents.

Mr./Ms. <<ISSA Chapter President>>,
I'm an Ohio State MIS & Accounting student working on an undergraduate thesis project concerning computer security vulnerability information. I received your e-mail address from the ISSA web site. For my project, I wish to distribute a link to an on-line survey via e-mail. I am inquiring as to whether you may distribute my e-mail to your ISSA chapter members. I have received cooperation from the local Columbus, OH ISSA chapter to send my survey link to members. However, I am attempting to survey those in the IT security field on a national level. I have already distributed my survey to InfraGard coordinators nationwide for distribution to members. I would be interested to see if the two groups of IT professionals hold different views.

The results of this survey will be used to support my undergraduate thesis project so I may graduate "with distinction" in MIS. The purpose of this research is to examine the public availability of computer security vulnerability information. With the risk that this information leads to an increased number of security breaches, I am attempting to examine the benefits of full disclosure. I'm also attempting to clarify what is ethical behavior in the wake of discovering a computer security vulnerability. I am completing this project under the supervision of Professor Richard Murdock from the OSU Accounting & MIS department. He may be reached at murdock.3@osu.edu or 292-1720.

My survey may be accessed at:
http://fisher.osu.edu/people/goens_1/osustudentproject.htm

I will be collecting survey responses up until March 10, 2001. I would deeply appreciate your support in forwarding this link to your members. I would be more than happy to share the results of this survey when my project is complete.

Sincerely,
Tami Goens
BSBA MIS & Accounting 6/01
The Ohio State University
goens.1@osu.edu
home 614.421.0318
cell 614.264.8153

Dr. Richard Murdock
Thesis Advisor
Professor, Ohio State University
Accounting & MIS Department
murdock.3@osu.edu
office 614.292.1720

APPENDIX C

Below are excerpts from selected e-mails received during the course of this study.

A. BugTraq subscribers on the sample selection...

"I wish I lived in a world where the only people graduating "with distinction" were those who had learned how silly results based on self-selected samples are. Evidentally, I don't."

"The bugtraq crowd is sure to be more in favor of full-disclosure than average"

"Do you expect this poll to generate an unbiased sample?"

"I'm not certain you'll have much statistically relevant data collected from the survey. The participants of your survey would seem to be coming from a segment of the population which already has a particular bias towards full disclosure (hence their membership to the bugtraq mailing list)"

"I would expect that the responses you get from a Security Focus mass mailing are considerably different than those from, say, a Micro$oft Users Group, the Privacy Foundation, or the ever-popular Midge Ure fan club."

"A self-selected survey has little to no statistical value. You have an extremely skewed sample by selecting for not just subscribers to BUGTRAQ, but subscribers to BUGTRAQ who might take the time to fill out your survey. Any conclusions you draw from the collected data should carefully note that you are using a biased sample."

B. Linux and text-only browser users on the survey platform...

"FYI:

This URL is unreadable under standard HTML 1.0. In other words it is unreadable in a text mode browser. I would be happy to complete the survey once it has been presented according to HTML 1.0 or optionally 1.1 standards (see RFC 1945 and/or 2068)"

"Your survey doesn't work with Lynx."

"Is there any reason for the page to be not readable with lynx? I would assume that many of the people you are targeting would be more used to the console...."

"Your survey is exceedingly unusable under Lynx.
You should design a more generally usable survey next time."

"I was unable to participate in your survey and I feel I should inform you why. A large number of bugtraq subscribers still use console mail apps like mutt and pine to read their mail. Additionally, they use lynx and other non_GUI browsers. By designing your page to be incompatible with such tools, I feel you exclude a segment of the BUGTRAQ readership that might otherwise respond, and may impact the validity of your results."

"With some difficulty I managed to finally navigate my way thru your non-text-browser-friendly site and filled out your survey.

I think you'll find that I'm not the only one. Many people on the "pointy end" of system security, especially those is Unix environments use text-friendly browsers like lynx and text email readers like pine, eschewing Microsoft products as much as possible."

C. On the use of JavaScript...

"It does not show much acumen within the security community to require users to enable scripting or to "hand check" the script code on the "accept the conditions" page, particularly when the desired effect can be obtained with pure HTML constructs."

"... [Y]ou used JavaScript. How many security professionals do you think will go to a foreign site with that turned on? In any event, you could have used a standard hyperlink, for all that the JavaScript was doing."

"You do not really expect security aware people to enable JavaScript in their browsers, do you?"

"Your request would be honored by me if your website would not request the activation of JavaScript. Any form of scripting in browsers is disabled in my office for security reasons. You might find out that more BugTraq readers are doing so. This might result in the fact that the most security minded people cannot complete the survey. And that is statistically not good for your survey;-)."

"Sorry, I cannot fill out your questionnaire because I have disabled JavaScript. For security reasons, you know. :-)"

"I find it ironic that JavaScript is required to complete your security survey."

"I wanted to complete your survey, but as I'm a security aware 'surfer', JavaScript etc. is disabled in my browser settings. I think this will be the case for many BugTraq subscribers, due to i.e. the frequent warnings from Georgi Guninski and others. So I can't see the consent dialog box. I think it would be a good idea to develop a html only version of the survey."

"Sadly, your questionnaire laced with JavaScript, which doesn't go through a number of the more paranoid firewall HTTP filters. Any chance you could remove the JavaScript requirement?"

"Forcing security folks to use JavaScript/java is the wrong idea"

"I am annoyed that you needed JavaScript enabled to fill out this survey. A lot of security-minded people keep JavaScript turned off. I filled it out anyway."

"I, and almost certainly many other BugTraq subscribers, cannot abide unnecessary JavaScript. I would suggest that you rework your web page so as to remove it; you will very likely get a much better response if you do."

"I would recommend removing the JavaScript popup ("consent dialog box) that first appears, as in my browser (Netscape/Linux) all of the text appeared on one (very) long line.

Visiting the site with JavaScript disabled presents the user with the text "consent dialog box please consent to participate in this study", without any actual means to consent, or to participate.

Making your site more accessible would go a long way towards encouraging people to fill in your questionnaire."

D. On the wording of the questions...

"The intent of questions nine and ten are not clear to me."

"I think that question #10 could be worded much more clearly than it is. Also, my answer would be different if the same question were asked once for black hats and once for script kiddies."

"I will not be answering your survey because it is imprecise and reflects careless design... 'Hacker websites' is a vague phrase, as the term 'hacker' has many different meanings depending on context and culture. Questions 8 and 9 are so vague as to be unanswerable. In question 8, what sort of 'vulnerability information' are we talking about? What is the baseline for the risk assessment? In question 9, what sort of risk are we talking about at all? I cannot guess it."

"Question 9 is incomplete so I assumed the rest of the question and answered accordingly... and Question 16 asks for a timeframe yet gives 'disagree, agree' etc so I didn't answer that one.

I have a remark on question 9: I do not fully understand the question (I am not a native English speaker). You might want to phrase it differently and specify what risk you are thinking of."

"> 8. On a scale of 1-10, with 10 being the strongest, I would assess
> the risk that publicly available vulnerability information will
> lead to an increased number of security breaches as a

An increased number of breaches as compared to *what*? The answer varies based on the missing portion of the question. e.g.,

As compared to the number of breaches if nobody released any security information? Yes, more information leads to more breaches.

As compared to the number of breaches if security information is out there, but just not on public lists/sites to which everyone has access? [probably about the same number, actually]

The interesting data point, however, isn't the total number of breaches, but the distribution of the breaches. More public information may lead to a greater sheer number of breaches, but these breaches will be among sites that do not use the information to mitigate risk. This allows sites with critical assets (e.g., financial institutions) reduce their risk, even if the risk for others may increase as a result.

> 9. On a scale of 1-10, with 10 being the strongest, I would assess
> the risk to those employed in computer security of not disclosing a
> vulnerability as a

It's not clear what you're trying to ask. Which risk are you concerned about? I can think of several off the top of my head:

* The risk that they won't have a job if there isn't a constant flow of vulnerabilities?

* The risk that customers won't see the need to spend on security without disclosure?

* The risk of not knowing what vulnerabilities actually exist (which is really a risk to their employer/customer, right?)?

> 16. Assuming a vulnerability is reported to a vendor, if that vendor
> does not address the reported vulnerability in what you consider a
> reasonable amount of time, that vulnerability should be made public.

The possible answers (Strongly Disagree -> Strongly Agree) don't match the question (e.g., 5 days, 10 days, 30 days, 6 mos, 1 year?)"

"The survey needs to be reworded.

You don't define 'full disclosure' but use the phrase several times. You don't distinguish between *vendors* doing the disclosure and *discoverers of the hole* doing the disclosure although this is a huge difference.

It's not clear whether 'vendors' refers to vendors in general, or vendors selling the particular product with a security vulnerability.

'vendor benefit' is a really broad issue - I would argue that vendors benefit in some ways but are hurt in other ways.

Question 8 is difficult to parse - are we asked to asses the severity of the risk to computers, or the amount of increased risk, or the count regardless of severity?

Question 9 doesn't make a lot of sense - risk to whom? To each other?

I can't parse Question 10.

There are also several negative questions - 'not x', 'less y'. These are really tough for non-native speakers."

"... [Y]ou grouped Black hatters and S'kiddies, I would treat those separately. There is a big difference, Black Hatters write their own code and are more dangerous than Script Kiddies. Even though there have been recent incidents involving Script Kiddies, I do not believe the threat is the same between the two."

"I don't think your questions are worded very well. I attempted to take the survey but after having to read the questions over and over again and still not knowing what you are asking, I gave up."

"One detail which I found off-putting: you phrase the last question (assuming you're not randomizing from a pool of questions or something like that; if you are, it's the one about benefit of an ethical code of conduct) as something to the effect of professionals in the business would benefit from an ethical code. "Would" implies that we don't currently have any such code, a characterization I'd strongly disagree with...."

E. Selected positive and insightful comments on the study...

"Good to see a creative topic like this drawing upon the resources of such community-driven entities as BugTraq. Keep up the good work!"

"I commend you for taking such a volatile topic for your thesis. It's an important topic, but so many people just prefer not to talk about it."

"...I've been wondering what people thought for some time..."

"Thank you for doing research on this extremely important topic. It has recently come to a head in the security scene, due partly, I think, to Marcue Ranum's keynote at July's Blackhat. I was there and was somewhat dismayed (not "disgusted", as many of my colleagues were), but also intrigued because many of his points were indeed legitimate. I didn't agree with the conclusions he drew from them, but the thoughts were important in that they started the recent debate on this topic."

"I'm against publicizing exploit scripts as a general rule. However, it helped us (at one of my clients) stop the ILOVEYOU worm before we had an updated signature file from our AV vendor. Our Outlook app was back up and running within a few hours after we had literally unplugged the cable from the back of the mail server to stop the initial attack...Again, it was an excellent survey - and I'd love to see the results!"

"...My experience leans towards full disclosure. Timing of the disclosure may display wisdom. Patching a vulnerability in a timely manner would seem prudent before global disclosure. In the world of hacking it is only a matter of time before a vulnerability is found and exploited. (Knowledge is Power, better forewarned sooner, than later.)

I believe that Security professionals have a code of ethics. We are trusted employees. Whether written or assumed the effect is the same. 'Trust once violated, is rarely regained.'

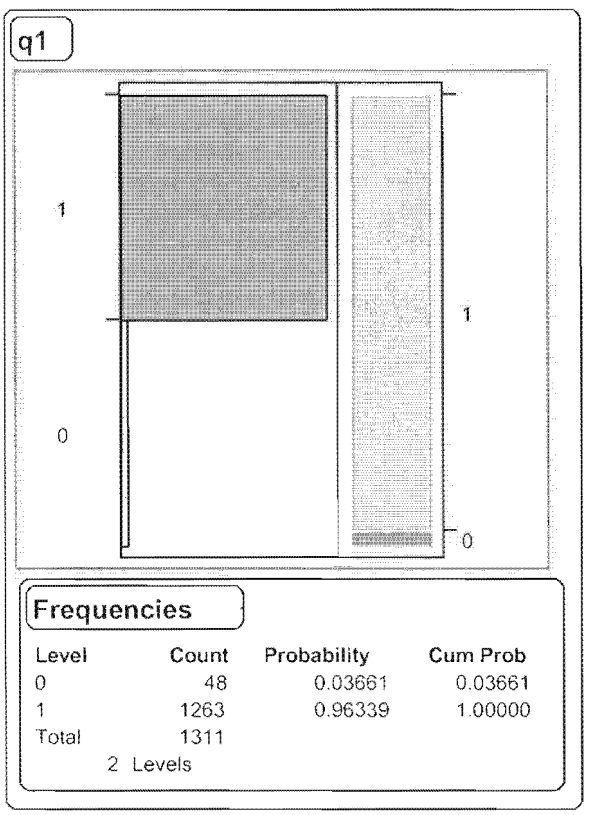
In the global world of information there is no one source for answers. The future security professional must continually be seeking sites and locations that can provide knowledge and insights into protecting their domains. Follow the leads whereever they are. (One must never be so indulged that caution is averted, since all information is not truly knowledge.)

I admire your courage to enter a profession that is needed so badly, understood so poorly and supported so casually be those that need your services the most. Continue on... break new ground, make new discoveries and improve upon that which has already been accomplished. Pioneers, we all are!"

APPENDIX D

SURVEY RESULTS

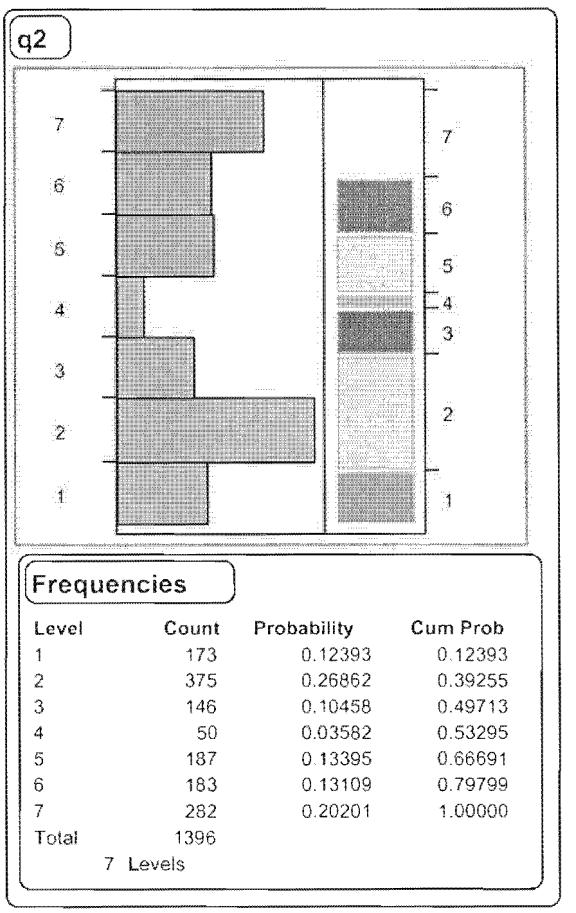
Question 1: Are you responsible for computer or network security in any way?
0=no
1=yes



	BugTraq	ISSA	InfraGard	
0	42	3	3	**48**
1	1142	54	67	**1263**
	1184	**57**	**70**	**1311**

Question 2: What is your primary job title?

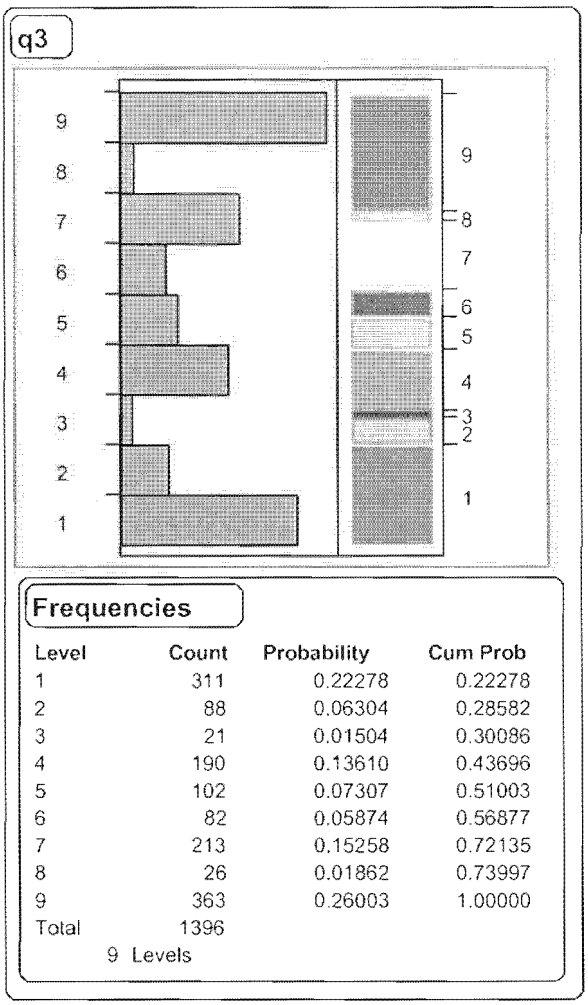
1=IS Management
2=Network Security Administrator/Mangement
3=Network Security Analyst
4=Systems Integrator
5=Consultant
6=Programmer
7=Other



	BugTraq	ISSA	InfraGard	
1	138	11	24	**173**
2	348	9	18	**375**
3	129	9	8	**146**
4	48	1	1	**50**
5	157	19	11	**187**
6	181	2	0	**183**
7	259	9	14	**282**
	1260	**60**	**76**	**1396**

Question 3: What is the primary industry of your organization?

1=Consulting Services
2=Consumer Products
3=Health Care
4=Education
5=Financial Services
6=Government
7=Telecommunications
8=Utilities
9=Other



Frequencies

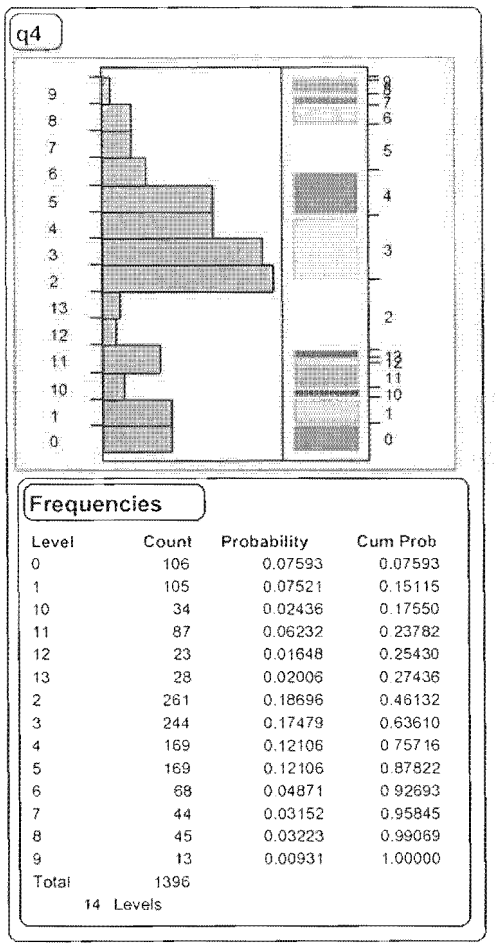
Level	Count	Probability	Cum Prob
1	311	0.22278	0.22278
2	88	0.06304	0.28582
3	21	0.01504	0.30086
4	190	0.13610	0.43696
5	102	0.07307	0.51003
6	82	0.05874	0.56877
7	213	0.15258	0.72135
8	26	0.01862	0.73997
9	363	0.26003	1.00000
Total	1396		

9 Levels

	BugTraq	ISSA	InfraGard	
1	274	21	16	**311**
2	81	2	5	**88**
3	16	2	3	**21**
4	184	1	5	**190**
5	85	5	12	**102**
6	59	7	16	**82**
7	205	2	6	**213**
8	18	4	4	**26**
9	338	16	9	**363**
	1260	**60**	**76**	**1396**

Question 4: How many years have you been working with computer security?

0=under 1 year
1=1 year
2=2 years
3=3 years
4=4 years
5=5 years
6=6 years
7=7 years
8=8 years
9=9 years
10=10 years
11=10-15 years
12=15-20
13=20+ years



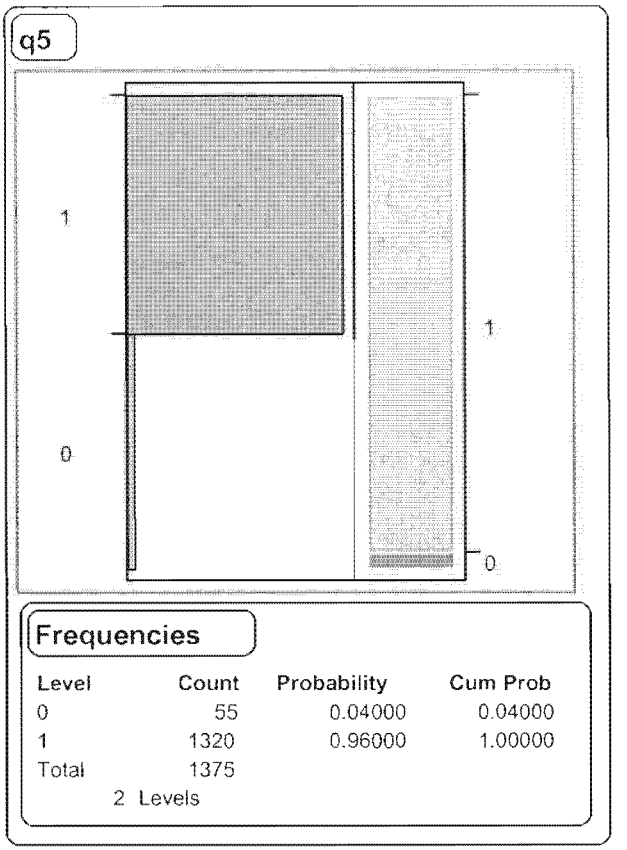
Level	Count	Probability	Cum Prob
0	106	0.07593	0.07593
1	105	0.07521	0.15115
10	34	0.02436	0.17550
11	87	0.06232	0.23782
12	23	0.01648	0.25430
13	28	0.02006	0.27436
2	261	0.18696	0.46132
3	244	0.17479	0.63610
4	169	0.12106	0.75716
5	169	0.12106	0.87822
6	68	0.04871	0.92693
7	44	0.03152	0.95845
8	45	0.03223	0.99069
9	13	0.00931	1.00000
Total	1396		

14 Levels

	BugTraq	ISSA	InfraGard	
0	99	1	6	**106**
1	99	5	1	**105**
2	249	6	6	**261**
3	226	4	14	**244**
4	164	2	3	**169**
5	152	10	7	**169**
6	64	3	1	**68**
7	38	2	4	**44**
8	36	3	6	**45**
9	10	0	3	**13**
10	27	1	6	**34**
11	71	9	7	**87**
12	12	8	3	**23**
13	13	6	9	**28**
	1260	**60**	**76**	**1396**

Question 5: Are you male or female?

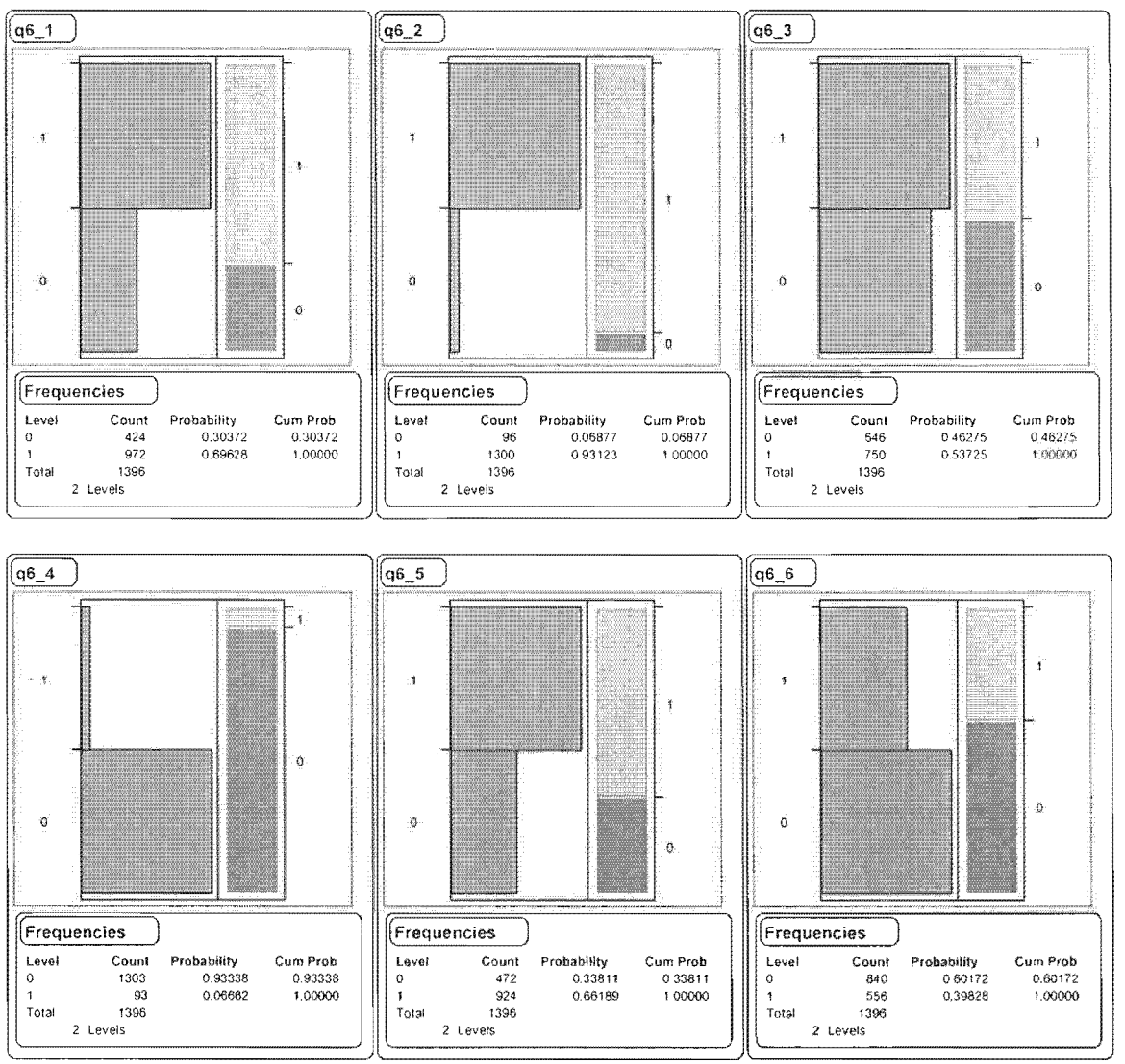
0=female
1=male



	BugTraq	ISSA	InfraGard	
0	36	7	12	**55**
1	1203	53	64	**1320**
	1239	**60**	**76**	**1375**

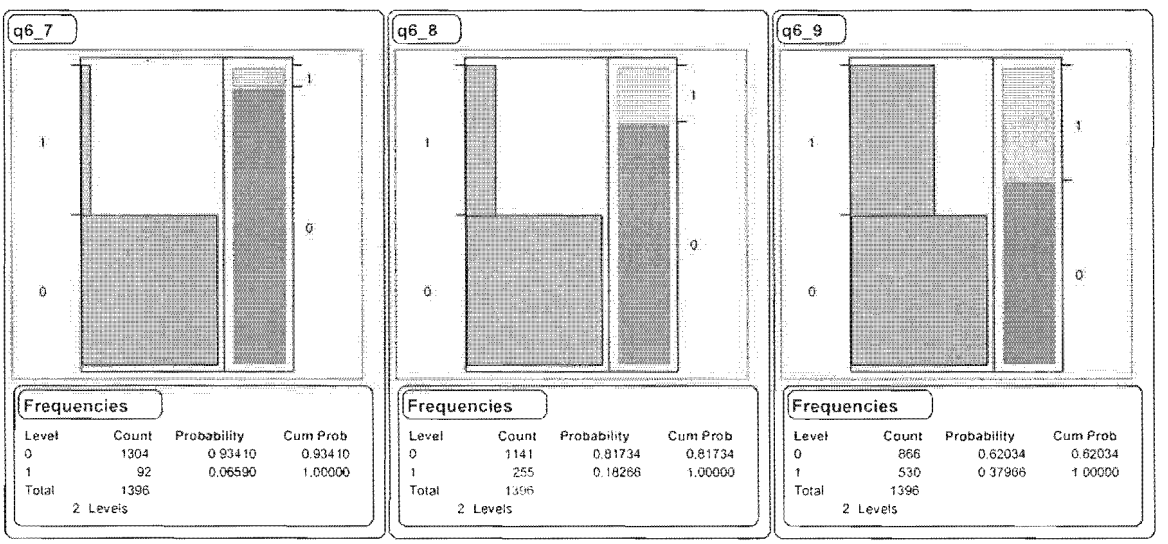
Question 6: What security vulnerability sources do you regularly monitor or use? (results for all three target groups combined)

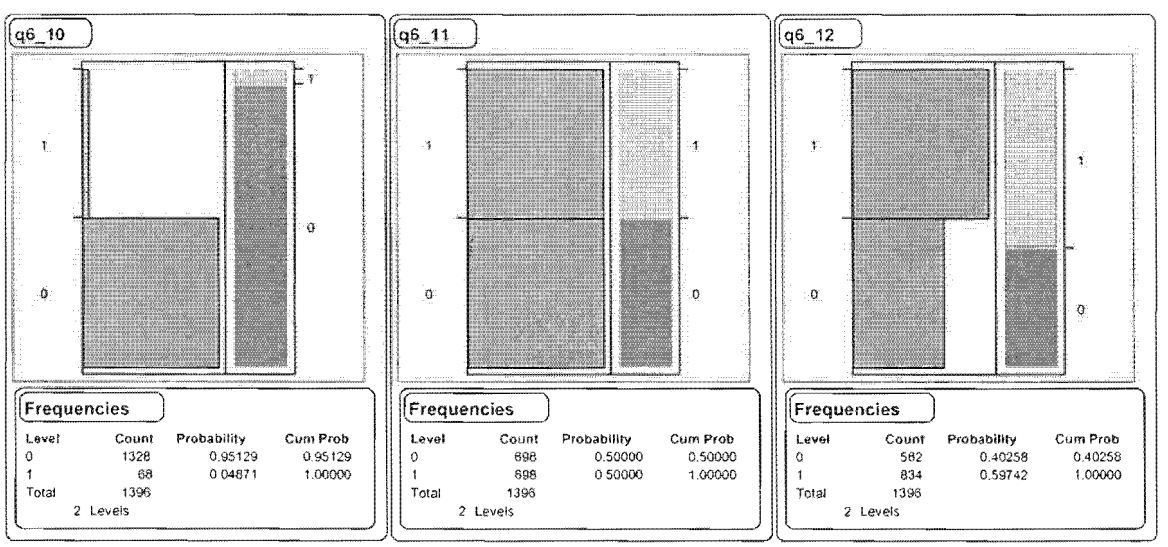
1=Securityfocus.com
2=Securityfocus.com mailing lists (BugTraq, NT BugTraq, focus –linux, etc.)
3=other mailing lists or newsgroups
4=NIST's ICAT database
5=CERT alerts
6=SANS security digest
7=NIPC Cybernotes
8=CIAC bulletins
9=Packetstorm
10=E-security Online
11=Vendor websites
12=Hacker websites
13=Other websites
14=Security audit services
15=Professional member security organization
16=Private security vulnerability information service provider
17=Other



Question 6 (continued): What security vulnerability sources do you regularly monitor or use?

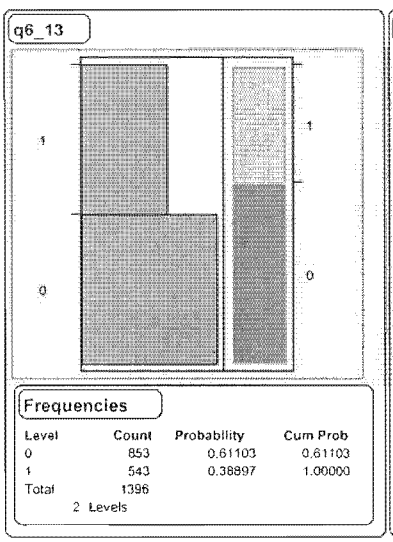
1=Securityfocus.com
2=Securityfocus.com mailing lists (BugTraq, NT BugTraq, focus –linux, etc.)
3=other mailing lists or newsgroups
4=NIST's ICAT database
5=CERT alerts
6=SANS security digest
7=NIPC Cybernotes
8=CIAC bulletins
9=Packetstorm
10=E-security Online
11=Vendor websites
12=Hacker websites
13=Other websites
14=Security audit services
15=Professional member security organization
16=Private security vulnerability information service provider
17=Other

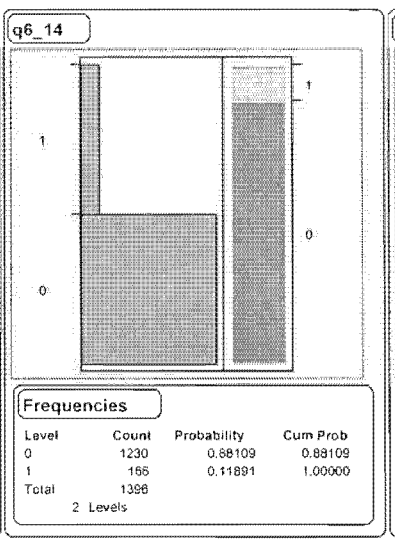


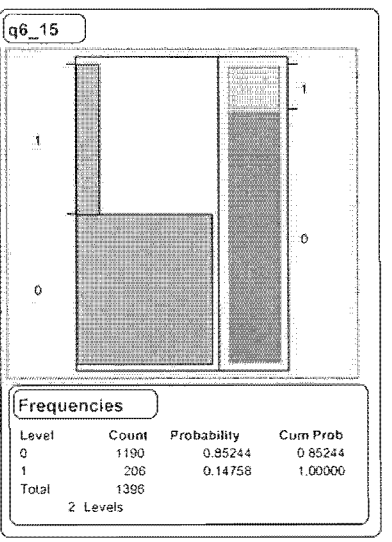


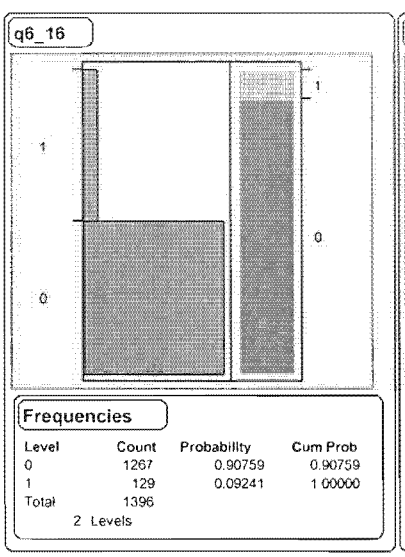
Question 6 (continued): What security vulnerability sources do you regularly monitor or use?

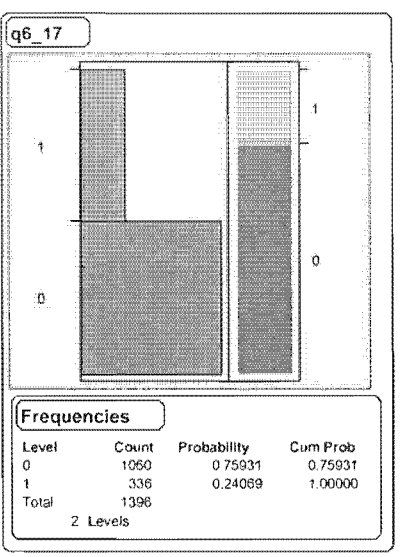
1=Securityfocus.com
2=Securityfocus.com mailing lists (BugTraq, NT BugTraq, focus –linux, etc.)
3=other mailing lists or newsgroups
4=NIST's ICAT database
5=CERT alerts
6=SANS security digest
7=NIPC Cybernotes
8=CIAC bulletins
9=Packetstorm
10=E-security Online
11=Vendor websites
12=Hacker websites
13=Other websites
14=Security audit services
15=Professional member security organization
16=Private security vulnerability information service provider
17=Other











Question 6 (continued): What security vulnerability sources do you regularly monitor or use?

Results broken down by target group:

Q6_1: Securityfocus.com				
	BugTraq	ISSA	InfraGard	
0 (no)	346	29	49	424
1 (yes)	914	31	27	972
	1260	60	76	1396

Q6_2: Securityfocus.com mailing lists (such as BugTraq, etc.)				
	BugTraq	ISSA	InfraGard	
0 (no)	30	30	36	96
1 (yes)	1230	30	40	1300
	1260	60	76	1396

Q6_3: Other mailing lists or newsgroups				
	BugTraq	ISSA	InfraGard	
0 (no)	575	22	49	646
1 (yes)	685	38	27	750
	1260	60	76	1396

Q6_4: NIST's ICAT database				
	BugTraq	ISSA	InfraGard	
0 (no)	1188	48	67	1303
1 (yes)	72	12	9	93
	1260	60	76	1396

Q6_5: CERT alerts				
	BugTraq	ISSA	InfraGard	
0 (no)	434	16	22	472
1 (yes)	826	44	54	924
	1260	60	76	1396

Question 6 (continued): What security vulnerability sources do you regularly monitor or use?

Results broken down by target group:

Q6_6: SANS security digest				
	BugTraq	ISSA	InfraGard	
0 (no)	791	14	35	840
1 (yes)	469	46	41	556
	1260	60	76	1396

Q6_7: NIPC Cybernotes				
	BugTraq	ISSA	InfraGard	
0 (no)	1202	53	49	1304
1 (yes)	58	7	27	92
	1260	60	76	1396

Q6_8: CIAC bulletins				
	BugTraq	ISSA	InfraGard	
0 (no)	1039	42	60	1141
1 (yes)	221	18	16	255
	1260	60	76	1396

Q6_9: Packetstorm				
	BugTraq	ISSA	InfraGard	
0 (no)	749	46	71	866
1 (yes)	511	14	5	530
	1260	60	76	1396

Q6_10: E-security Online				
	BugTraq	ISSA	InfraGard	
0 (no)	1209	50	69	1328
1 (yes)	51	10	7	68
	1260	60	76	1396

Question 6 (continued): What security vulnerability sources do you regularly monitor or use?

Results broken down by target group:

Q6_11: Vendor websites				
	BugTraq	ISSA	InfraGard	
0 (no)	635	30	33	698
1 (yes)	625	30	43	698
	1260	60	76	1396

Q6_12: Hacker websites				
	BugTraq	ISSA	InfraGard	
0 (no)	486	32	44	562
1 (yes)	774	28	32	834
	1260	60	76	1396

Q6_13: Other websites				
	BugTraq	ISSA	InfraGard	
0 (no)	766	37	50	853
1 (yes)	494	23	26	543
	1260	60	76	1396

Q6_14: Security audit services				
	BugTraq	ISSA	InfraGard	
0 (no)	1117	52	61	1230
1 (yes)	143	8	15	166
	1260	60	76	1396

Q6_15: Professional member security organization				
	BugTraq	ISSA	InfraGard	
0 (no)	1137	15	38	1190
1 (yes)	123	45	38	206
	1260	60	76	1396

Question 6 (continued): What security vulnerability sources do you regularly monitor or use?

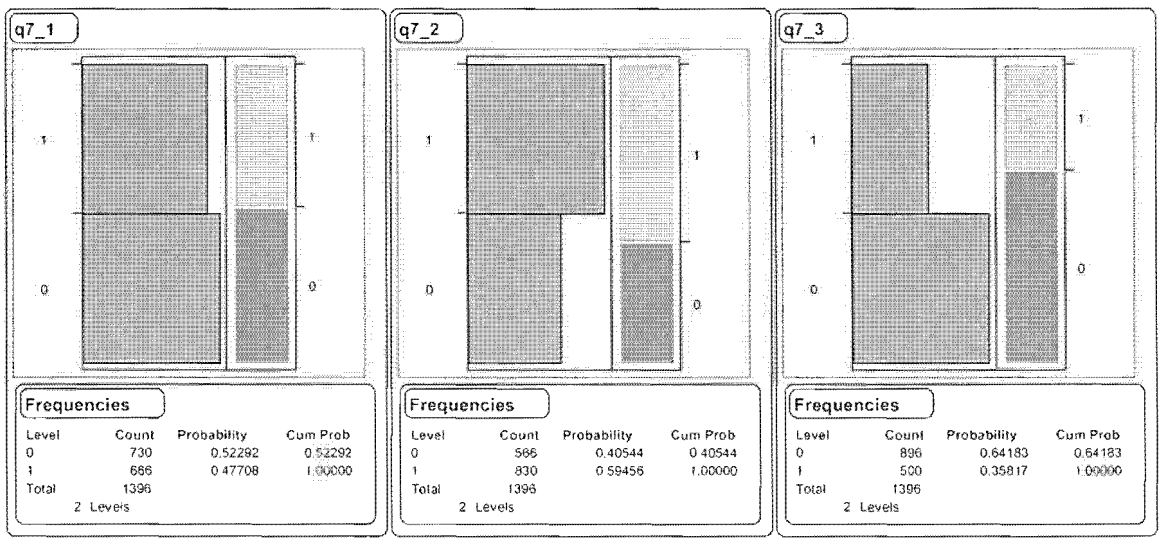
Results broken down by target group:

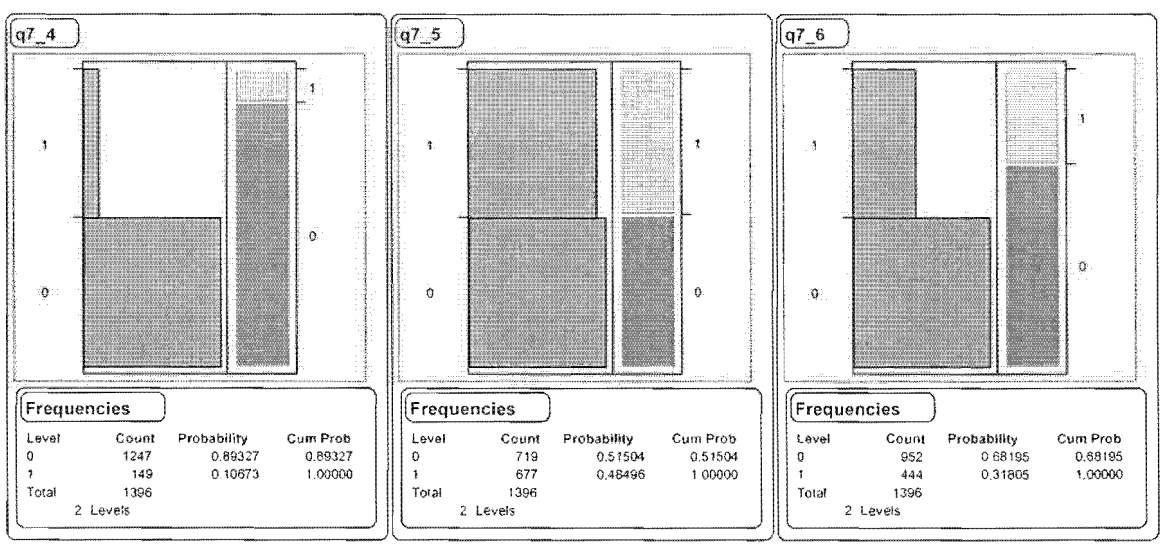
Q6_16: Private security vulnerability information service provider				
	BugTraq	ISSA	InfraGard	
0 (no)	1157	53	57	1267
1 (yes)	103	7	19	129
	1260	60	76	1396

Q6_17: Other				
	BugTraq	ISSA	InfraGard	
0 (no)	958	49	53	1060
1 (yes)	302	11	23	336
	1260	60	76	1396

Question 7 (continued): What sources are you aware of that others in your organization concerned with security vulnerabilities monitor or use?

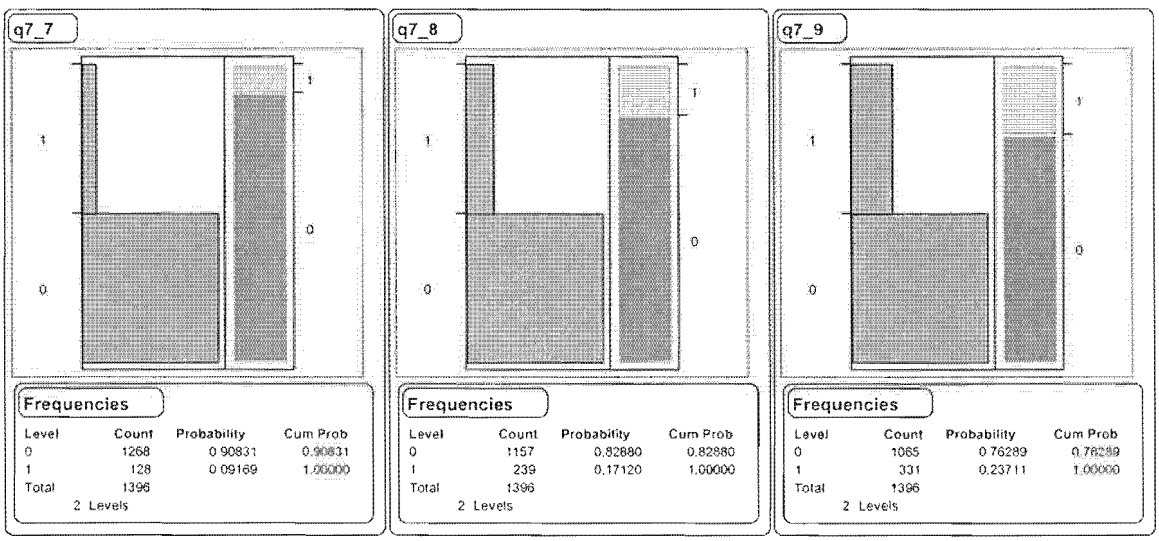
1=Securityfocus.com
2=Securityfocus.com mailing lists
(BugTraq, NT BugTraq, focus –linux, etc.)
3=other mailing lists or newsgroups
4=NIST's ICAT database
5=CERT alerts
6=SANS security digest
7=NIPC Cybernotes
8=CIAC bulletins
9=Packetstorm
10=E-security Online
11=Vendor websites
12=Hacker websites
13=Other websites
14=Security audit services
15=Professional member security organizatio
16=Private security vulnerability information service provider
17=Other

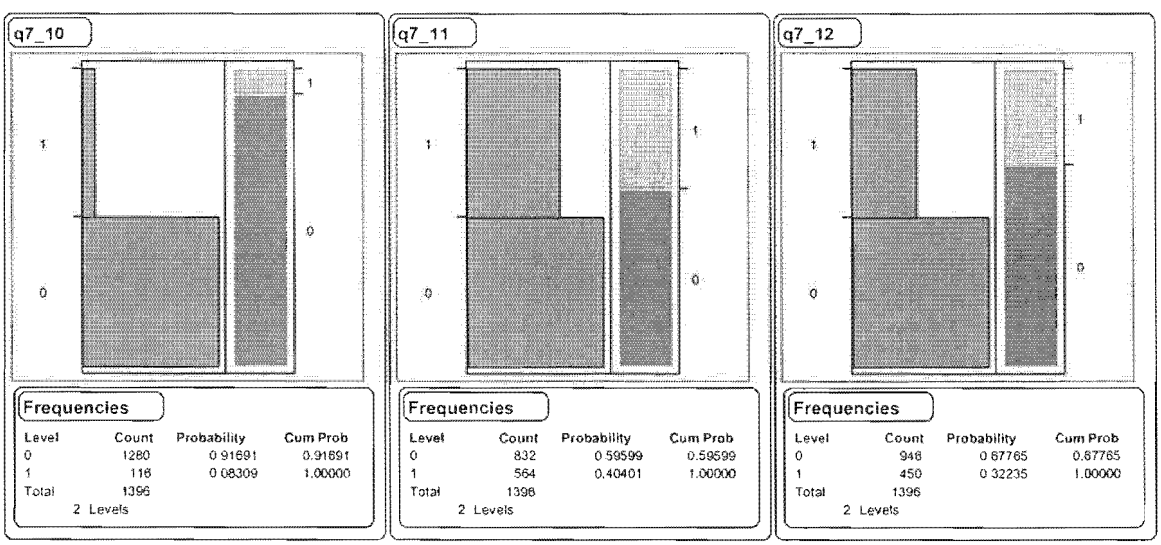




Question 7(continued): What sources are you aware of that others in your organization concerned with security vulnerabilities monitor or use?

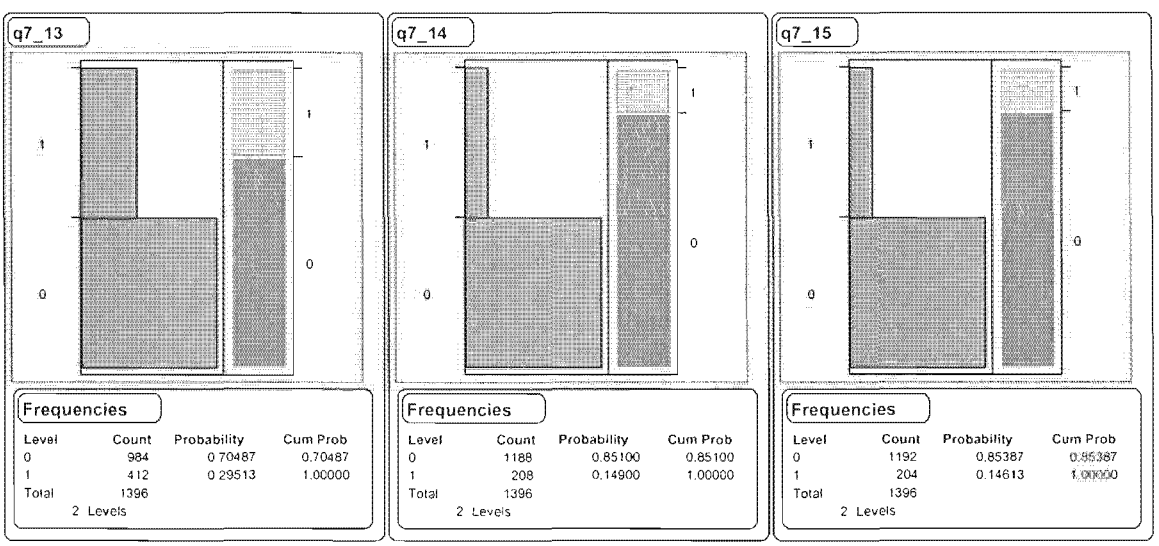
1=Securityfocus.com
2=Securityfocus.com mailing lists (BugTraq, NT BugTraq, focus –linux, etc.)
3=other mailing lists or newsgroups
4=NIST's ICAT database
5=CERT alerts
6=SANS security digest
7=NIPC Cybernotes
8=CIAC bulletins
9=Packetstorm
10=E-security Online
11=Vendor websites
12=Hacker websites
13=Other websites
14=Security audit services
15=Professional member security organizatio
16=Private security vulnerability information service provider
17=Other

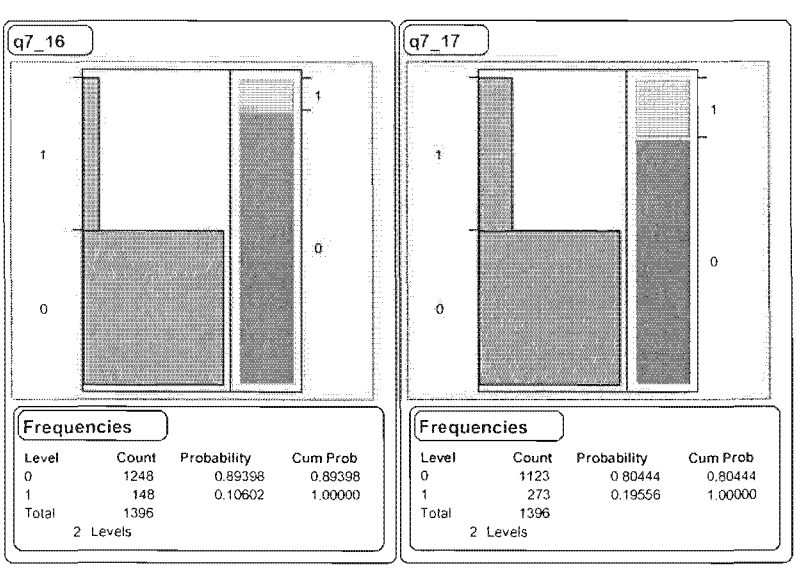




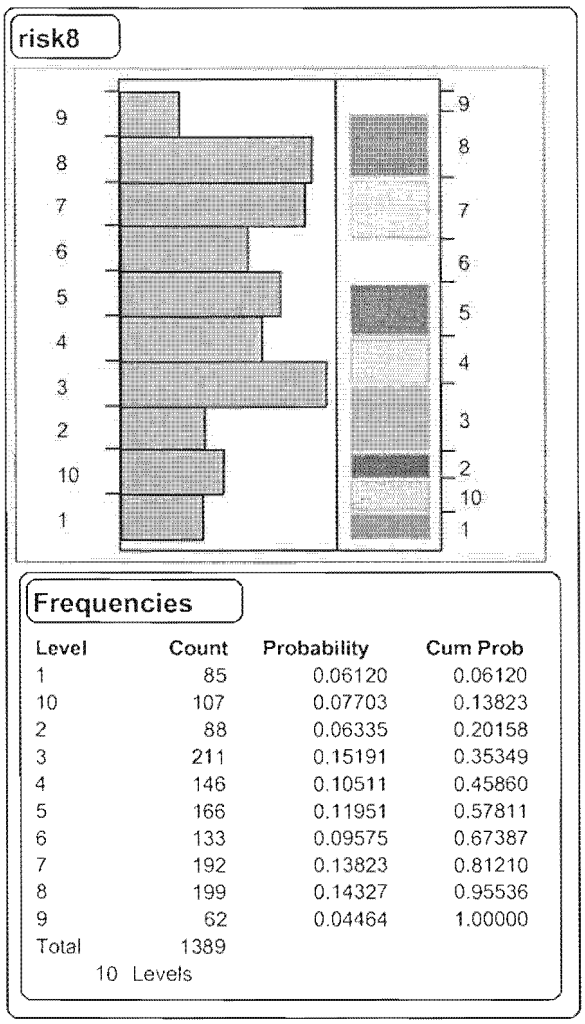
Question 7 (continued): What sources are you aware of that others in your organization concerned with security vulnerabilities monitor or use?

1=Securityfocus.com
2=Securityfocus.com mailing lists (BugTraq, NT BugTraq, focus –linux, etc.)
3=other mailing lists or newsgroups
4=NIST's ICAT database
5=CERT alerts
6=SANS security digest
7=NIPC Cybernotes
8=CIAC bulletins
9=Packetstorm
10=E-security Online
11=Vendor websites
12=Hacker websites
13=Other websites
14=Security audit services
15=Professional member security organizatio
16=Private security vulnerability information service provider
17=Other





Question 8: On a scale of 1-10, with 10 being the strongest, I would assess the risk that publicly available vulnerability information will lead to an increased number of security breaches as a (respondent given a 1-10 rating scale).



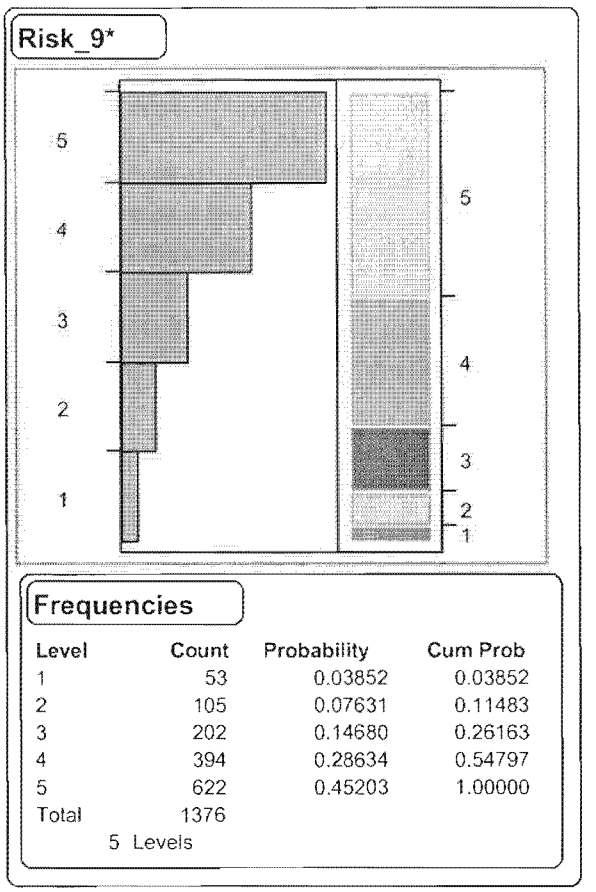
Level	Count	Probability	Cum Prob
1	85	0.06120	0.06120
10	107	0.07703	0.13823
2	88	0.06335	0.20158
3	211	0.15191	0.35349
4	146	0.10511	0.45860
5	166	0.11951	0.57811
6	133	0.09575	0.67387
7	192	0.13823	0.81210
8	199	0.14327	0.95536
9	62	0.04464	1.00000
Total	1389		

10 Levels

*	BugTraq	ISSA	InfraGard	
1	163	5	5	**173**
2	332	15	10	**357**
3	273	12	14	**299**
4	342	20	29	**391**
5	143	8	18	**169**
	1253	**60**	**76**	**1389**

* 1-10 rating scale collapsed to 1-5 scale as discussed in Chapter 3.

Question 9: On a scale of 1-10, with 10 being the strongest, I would assess the risk to those employed in computer security of not disclosing a vulnerability as a (respondent given a 1-10 rating scale).

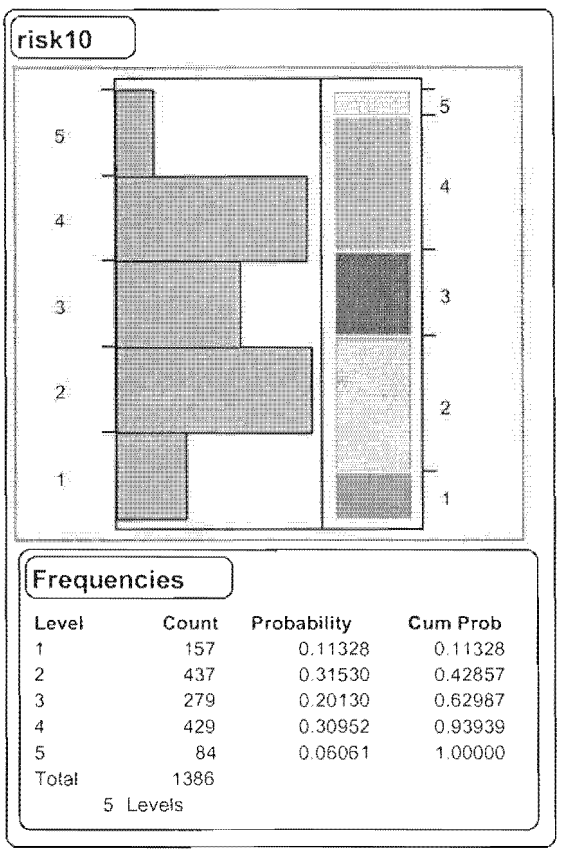


*	BugTraq	ISSA	InfraGard	
1	44	2	7	**53**
2	89	6	10	**105**
3	179	7	15	**201**
4	352	21	21	**394**
5	577	23	22	**622**
	1241	59	75	**1375**

* 1-10 rating scale collapsed to 1-5 scale as discussed in Chapter 3.

Question 10: Historical vulnerability information is less risky in the hands of black hat hackers and script kiddies than recently published vulnerability information. Respondent given the following options:

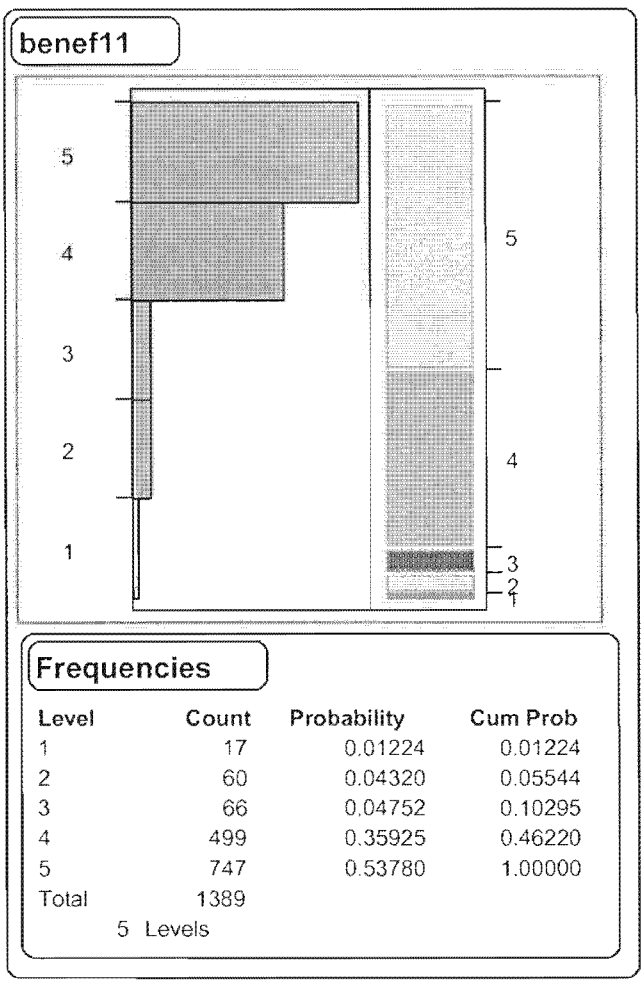
1=strongly disagree
2=disagree
3=neutral
4=agree
5=strongly agree



	BugTraq	ISSA	InfraGard	
1	140	8	9	**157**
2	383	28	26	**437**
3	253	10	16	**279**
4	397	11	21	**429**
5	78	2	4	**84**
	1251	**59**	**76**	**1386**

Question 11: Public disclosure of vulnerabilities results in more secure products from vendors.
Respondent given the following options:

1=strongly disagree
2=disagree
3=neutral
4=agree
5=strongly agree



Frequencies

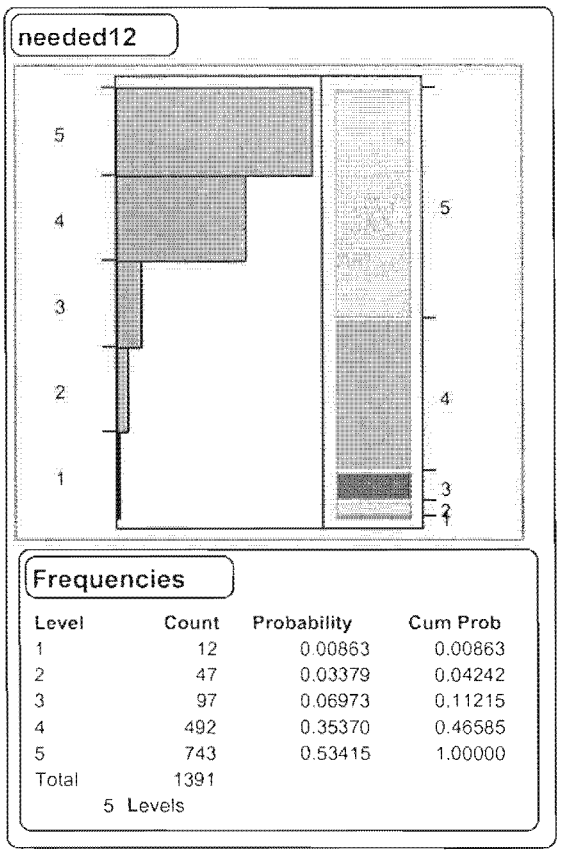
Level	Count	Probability	Cum Prob
1	17	0.01224	0.01224
2	60	0.04320	0.05544
3	66	0.04752	0.10295
4	499	0.35925	0.46220
5	747	0.53780	1.00000
Total	1389		

5 Levels

	BugTraq	ISSA	InfraGard	
1	15	1	1	**17**
2	44	3	13	**60**
3	56	5	5	**66**
4	432	29	38	**499**
5	706	22	19	**747**
	1253	**60**	**76**	**1389**

Question 12: Full disclosure of vulnerabilities is necessary for legitimate security purposes.
Respondent given the following options:

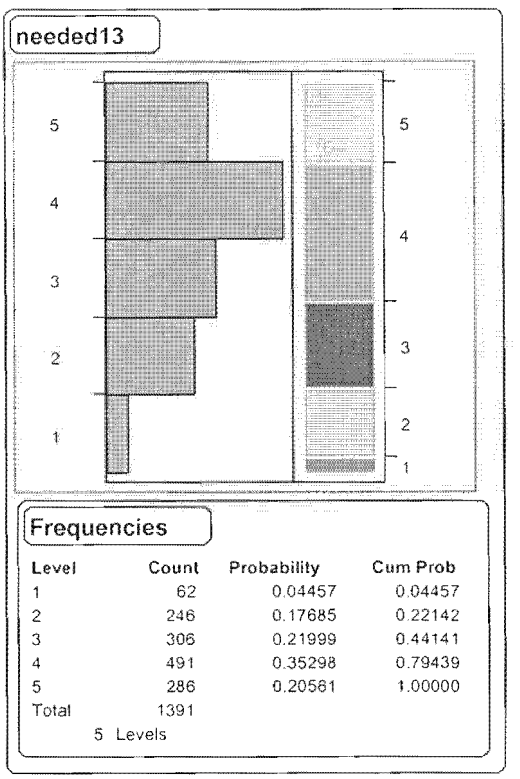
1=strongly disagree
2=disagree
3=neutral
4=agree
5=strongly agree



	BugTraq	ISSA	InfraGard	
1	9	1	2	**12**
2	29	7	11	**47**
3	79	7	11	**97**
4	433	26	33	**492**
5	705	19	19	**743**
	1255	**60**	**76**	**1391**

Question 13: Full disclosure of exploit code is necessary for legitimate security purposes.
Respondent given the following options:

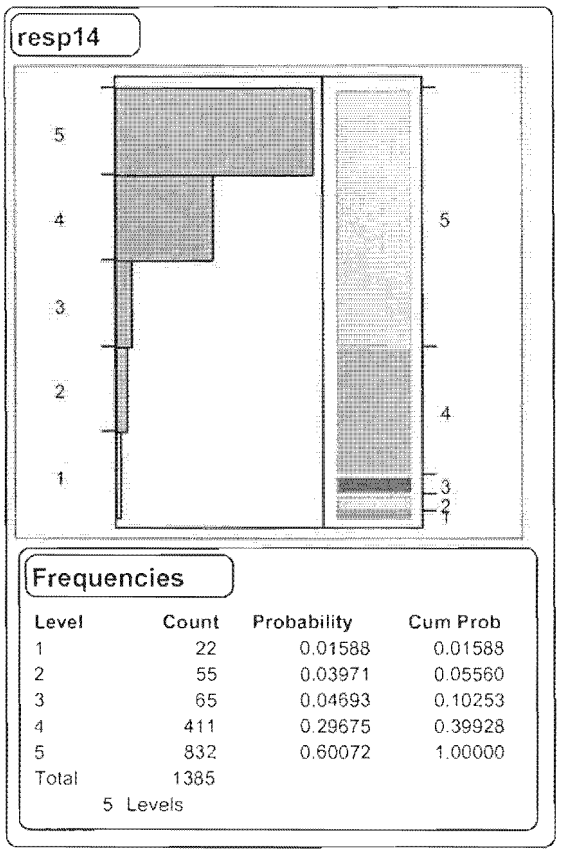
1=strongly disagree
2=disagree
3=neutral
4=agree
5=strongly agree



	BugTraq	ISSA	InfraGard	
1	54	3	5	**62**
2	206	18	22	**246**
3	280	12	14	**306**
4	453	18	20	**491**
5	262	9	15	**286**
	1255	**60**	**76**	**1391**

Question 14: A security professional has a responsibility to report discovered vulnerabilities to vendors.
Respondent given the following options:

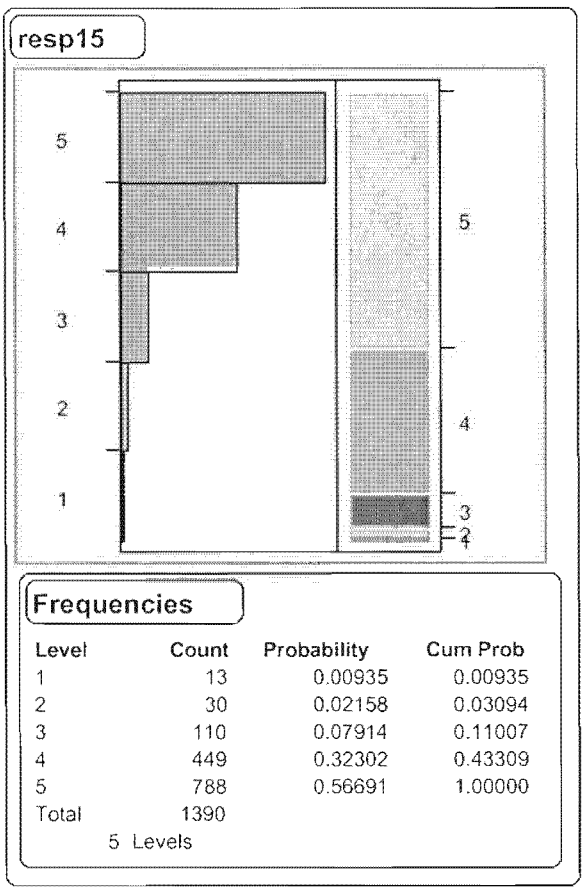
1=strongly disagree
2=disagree
3=neutral
4=agree
5=strongly agree



	BugTraq	ISSA	InfraGard	
1	22	0	0	**22**
2	52	0	3	**55**
3	57	4	4	**65**
4	369	24	18	**411**
5	749	32	51	**832**
	1249	**60**	**76**	**1385**

Question 15: A vulnerability should be reported to the vendor prior to disclosing the vulnerability to the public.
Respondent given the following options:

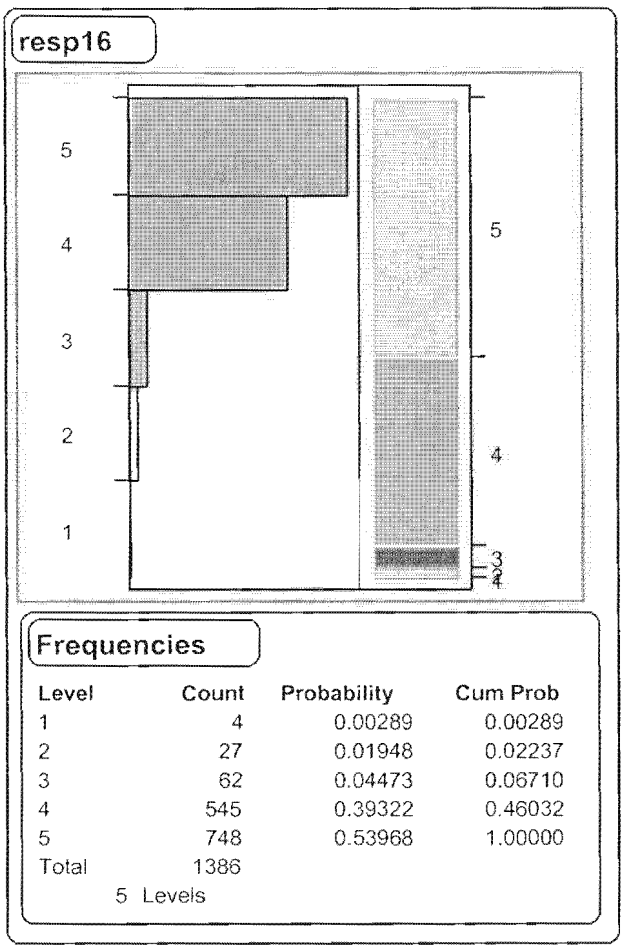
1=strongly disagree
2=disagree
3=neutral
4=agree
5=strongly agree



	BugTraq	ISSA	InfraGard	
1	13	0	0	**13**
2	29	0	1	**30**
3	98	7	5	**110**
4	408	16	25	**449**
5	707	36	45	**788**
	1255	**59**	**76**	**1390**

Question 16: Assuming a vulnerability is reported to a vendor, if that vendor does not address the reported vulnerability in what you consider a reasonable amount of time, that vulnerability should be made public.
Respondent given the following options:

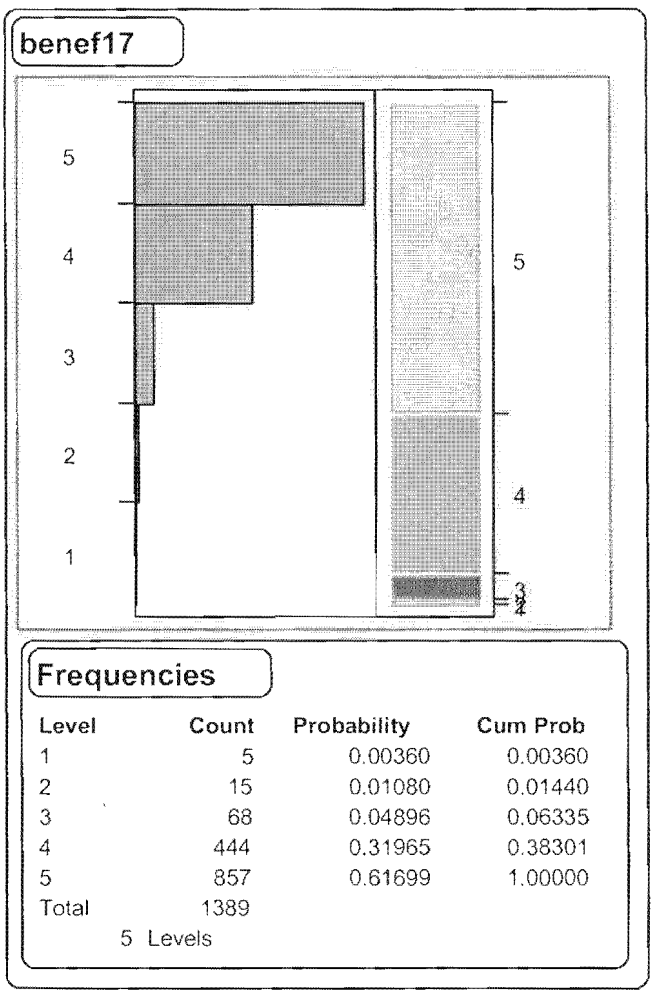
1=strongly disagree
2=disagree
3=neutral
4=agree
5=strongly agree



	BugTraq	ISSA	InfraGard	
1	2	0	2	**4**
2	17	4	6	**27**
3	47	8	7	**62**
4	475	24	46	**545**
5	710	23	15	**748**
	1251	**59**	**76**	**1386**

Question 17: Those employed in computer and network security have benefited from full disclosure.
Respondent given the following options:

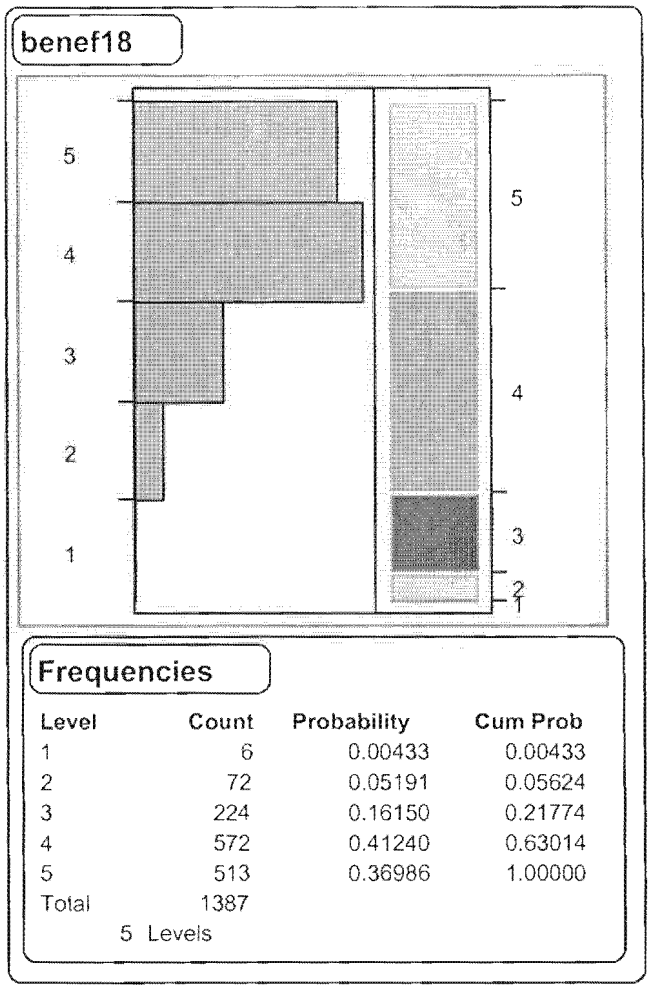
1=strongly disagree
2=disagree
3=neutral
4=agree
5=strongly agree



	BugTraq	ISSA	InfraGard	
1	4	0	1	**5**
2	9	4	2	**15**
3	49	7	12	**68**
4	379	24	41	**444**
5	812	25	20	**857**
	1253	**60**	**76**	**1389**

Question 18: Vendors have benefited from full disclosure.
Respondent given the following options:

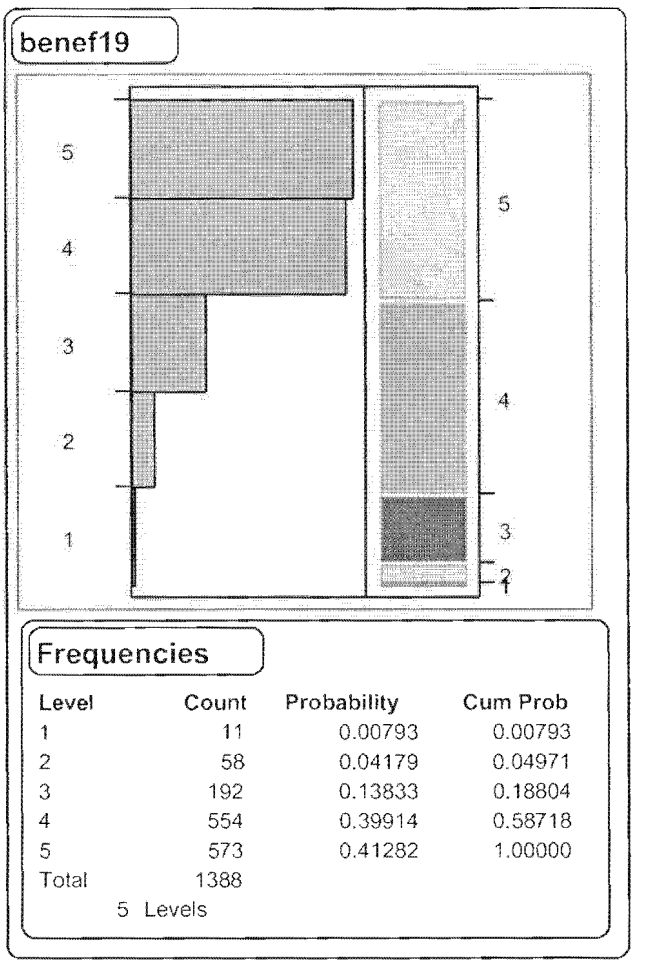
1=strongly disagree
2=disagree
3=neutral
4=agree
5=strongly agree



	BugTraq	ISSA	InfraGard	
1	5	0	1	**6**
2	62	4	6	**72**
3	201	17	6	**224**
4	501	23	48	**572**
5	482	16	15	**513**
	1251	**60**	**76**	**1387**

Question 19: Society as a whole has benefited from full disclosure.
Respondent given the following options:

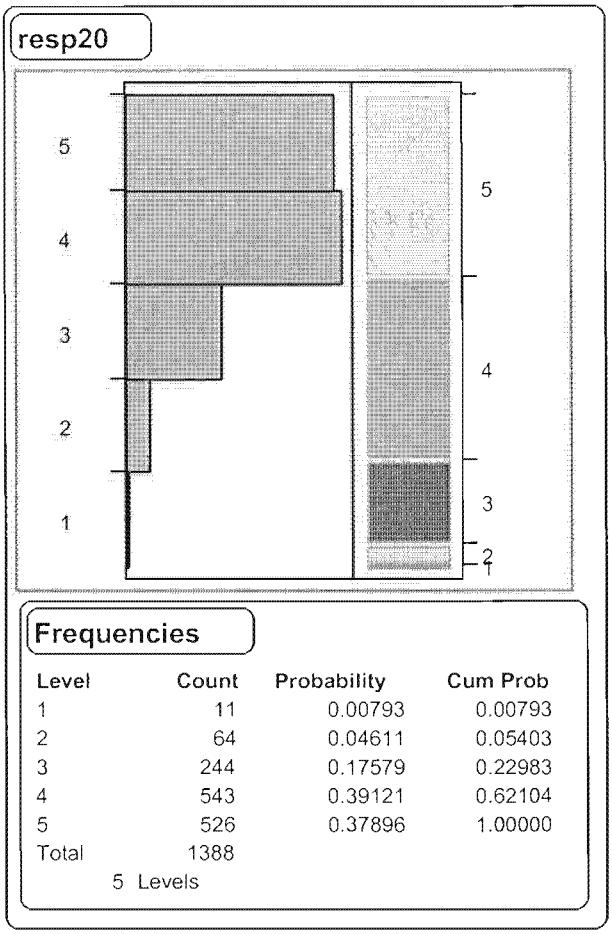
1=strongly disagree
2=disagree
3=neutral
4=agree
5=strongly agree



	BugTraq	ISSA	InfraGard	
1	9	0	2	**11**
2	44	6	8	**58**
3	163	11	18	**192**
4	490	29	35	**554**
5	546	14	13	**573**
	1252	**60**	**76**	**1388**

Question 20: Those employed in computer and network security would benefit from an ethical code of conduct.
Respondent given the following options:

1=strongly disagree
2=disagree
3=neutral
4=agree
5=strongly agree



	BugTraq	ISSA	InfraGard	
1	10	1	0	**11**
2	60	2	2	**64**
3	232	2	10	**244**
4	490	21	32	**543**
5	461	34	31	**526**
	1253	**60**	**75**	**1388**